



Honeywell Connected Life Safety Services CLSS Gateway

HON-CGW-MBB

Installation and Users' Manual

Table of Contents

| | |
|---|-----------|
| Section 1: General Information | 6 |
| 1.1: About This Manual | 6 |
| 1.2: Information Sources..... | 6 |
| 1.2.1: Training Modules..... | 6 |
| 1.2.2: Related Documents | 6 |
| 1.3: Documentation Feedback | 8 |
| 1.4: Revision History..... | 8 |
| 1.5: Abbreviations Used | 11 |
| 1.6: Approvals..... | 12 |
| 1.7: Warnings and Cautions in This Manual..... | 13 |
| 1.8: The Product Standards..... | 13 |
| 1.9: Disclaimer | 13 |
| Section 2: Overview | 14 |
| 2.1: Operation..... | 14 |
| 2.2: Honeywell Connected Life Safety Services..... | 14 |
| 2.3: Gateway Board Layout..... | 14 |
| 2.3.1: Connecting Interfaces..... | 15 |
| 2.3.2: LED Indicators | 16 |
| 2.3.3: Switches on the Gateway Board..... | 18 |
| 2.4: CLSS Gateway Parts | 18 |
| Section 3: Security Recommendations | 19 |
| 3.1: For Users..... | 19 |
| 3.2: For Preventing Potential Risks..... | 19 |
| 3.2.1: Unauthorized Access | 19 |
| User Access and Passwords..... | 19 |
| 3.2.2: Memory Media..... | 19 |
| 3.2.3: Software and Firmware Updates..... | 20 |
| 3.2.4: Viruses and Other Malicious Software Agents..... | 20 |
| 3.2.5: Network and Firewall Setup | 20 |
| Best Practices: Network Security..... | 21 |
| Best Practices: Connected Devices | 21 |
| 3.2.6: Securing the Monitoring Stations..... | 21 |
| Section 4: Installation | 22 |
| 4.1: Wall Mounting the Fixed Gateway..... | 22 |
| 4.2: Mounting the Portable Gateway | 24 |
| 4.2.1: Mounting onto the Chassis..... | 24 |
| 4.3: Gateway Board Connection Options..... | 25 |
| 4.3.1: Connecting to a Fire Alarm Panel..... | 26 |
| 4.3.2: Installing a Cellular Module..... | 26 |
| Compatibility Requirements | 26 |
| Before Installing a Cellular Module..... | 26 |
| Precautions for Service Quality | 26 |
| To Install a Cellular Module | 26 |
| Replacing the SIM Card..... | 27 |
| 4.3.3: Installing the External Aerials | 28 |
| To Install an External Antenna | 28 |
| Section 5: Configurations | 29 |
| 5.1: Commissioning the Gateway..... | 29 |
| 5.1.1: The Commissioning Steps..... | 29 |
| 5.1.2: Exporting Panel's Topology Data | 29 |
| To Export the Topology Data..... | 29 |
| 5.1.3: To Configure via the Wireless Connection | 29 |

| | |
|---|-----------|
| 5.2: Verifying the Gateway Connections..... | 32 |
| 5.3: Panel Brand and Connection Settings..... | 33 |
| 5.3.1: To Change the Connection Settings..... | 33 |
| 5.4: Honeywell CLSS Alarm Transmission Services..... | 34 |
| Communication Management..... | 34 |
| 5.4.1: Central Station Communication..... | 34 |
| 5.4.2: Activating the Central Station Communication..... | 34 |
| Adding a Central Station to the CLSS Account..... | 34 |
| Install a Fixed Gateway at the Site..... | 35 |
| Configuring the Central Station Communication..... | 35 |
| Verifying the Central Station Communication Configurations..... | 36 |
| 5.4.3: Dual Path Communication for Alarm Transmission..... | 36 |
| Supervision Period..... | 36 |
| Transmission Options..... | 36 |
| Section 6: Post-Installation Activities..... | 37 |
| 6.1: Upgrading the Gateway Firmware..... | 37 |
| 6.1.1: To Upgrade Before Commissioning the Gateway..... | 37 |
| 6.1.2: To Upgrade After Commissioning the Gateway..... | 38 |
| 6.1.3: To Locally Upgrade with a PC..... | 39 |
| 6.1.4: To Verify the Upgrade..... | 39 |
| 6.1.5: LED Indications During the Upgrade..... | 39 |
| 6.2: Troubleshooting..... | 40 |
| 6.2.1: To Troubleshoot LED-Indicated Issues..... | 40 |
| 6.2.2: To Troubleshoot Other Issues..... | 41 |
| Section 7: Modbus Communications..... | 43 |
| 7.1: Operation..... | 43 |
| 7.2: Functionality..... | 43 |
| 7.3: Recommended Cybersecurity Practices..... | 43 |
| 7.4: Required Software..... | 43 |
| 7.5: IP Requirements..... | 43 |
| 7.5.1: IP Port Settings..... | 43 |
| 7.5.2: IP Restrictions..... | 44 |
| 7.6: Bandwidth Calculation..... | 44 |
| Requirements for the Calculation..... | 44 |
| 7.7: System Architecture..... | 45 |
| 7.7.1: Redundancy..... | 47 |
| 7.8: Replacing the Modbus Gateway (Modbus-GW)..... | 48 |
| 7.9: Using Both the CLSS Gateway and the Modbus Gateway..... | 48 |
| 7.10: Agency Listings and Approvals..... | 49 |
| 7.10.1: Agency Restrictions and Limitations..... | 49 |
| 7.11: Standards..... | 49 |
| Underwriters Laboratories..... | 49 |
| Underwriters Laboratories Canada..... | 49 |
| National Fire Protection Association..... | 49 |
| Underwriters Laboratories Canada..... | 49 |
| 7.12: Compatible Equipment..... | 50 |
| 7.13: Modbus Feature Activation..... | 51 |
| 7.13.1: To Purchase the Modbus Support..... | 51 |
| 7.13.2: To Activate the Modbus Support..... | 52 |
| 7.14: Installation and Configurations..... | 53 |
| 7.15: The IP Settings..... | 53 |

| | |
|---|-----------|
| 7.16: To Connect with the Modbus Client | 53 |
| 7.17: To Configure the Modbus Settings | 54 |
| 7.18: To Configure the Modbus Client | 57 |
| 7.19: Modbus Command Support | 57 |
| Exception Responses | 57 |
| Modbus Addressing | 57 |
| 7.20: CLSS Gateway Control Features | 57 |
| 7.20.1: Supported Commands | 57 |
| 7.20.2: Enabling Control | 58 |
| 7.20.3: Sending Commands | 58 |
| 7.21: Analog Values and Trending | 59 |
| Analog Value Use Cases | 60 |
| 7.22: Register Mapping | 61 |
| 7.22.1: Register Mapping Overview | 61 |
| 7.22.2: Point Status Holding Registers | 61 |
| 7.22.3: Point Device Type Input Registers | 63 |
| 7.22.4: Zones/Panel Circuits Status Holding Registers | 64 |
| 7.22.5: Bell Circuits Status Holding Registers | 65 |
| 7.22.6: Bell Circuits Device Type Input Registers | 66 |
| 7.22.7: Panel Status Holding Register | 67 |
| 7.23: Analog Values Input Registers | 67 |
| 7.23.1: Panel and System Troubles Holding Registers | 67 |
| 7.23.2: Gateway Information Input Registers | 68 |
| 7.23.3: Node Status Details | 68 |
| 7.24: Read Device Identification (0x2B/0x0E) | 68 |
| 7.25: Troubleshooting | 69 |
| 7.25.1: What are some basic guidelines when installing a CLSS Gateway? | 69 |
| 7.25.2: How fast can the Modbus client poll the gateway? | 69 |
| 7.25.3: How can I tell if the gateway is running? | 69 |
| 7.25.4: How do I recover a lost password from the gateway? | 69 |
| 7.25.5: What is an “initialization read” for analog values? | 69 |
| 7.25.6: How many analog values can I read at a time? | 69 |
| 7.25.7: Why do I get an exception code when trying to read an analog value? | 69 |
| 7.25.8: Why do I get all zeros when I read an analog value? | 70 |
| 7.26: What is the “Analog Value Polling Time Out”? | 70 |
| 7.27: Conversion to Modbus RTU | 70 |
| 7.27.1: Hardware Configuration | 70 |
| 7.27.2: Software Configuration | 71 |
| 7.27.3: Connecting the Moxa MGate MB3180 Interface | 72 |
| 7.28: System Trouble | 73 |
| 7.29: Exception Responses | 73 |
| 7.30: CLSS Gateway Active Event Code | 74 |
| 7.31: Device Types | 75 |
| 7.32: System Troubles Register Map | 77 |
| Section 8: The BACnet Feature | 89 |
| 8.1: Agency Listings | 90 |
| 8.1.1: Compliance | 90 |
| National Fire Protection Association | 90 |
| Underwriters Laboratories | 90 |
| Underwriters Laboratories Canada | 90 |
| 8.2: Installation | 90 |
| Local | 90 |

| | |
|---|------------|
| Underwriters Laboratories | 90 |
| Underwriters Laboratories Canada | 90 |
| Canada | 90 |
| 8.3: Compatibility..... | 91 |
| 8.4: System Requirements..... | 91 |
| 8.5: System Architecture..... | 91 |
| 8.5.1: Single Panel Architecture..... | 91 |
| 8.5.2: NFN Network Architecture..... | 92 |
| 8.6: BACnet Feature Activation..... | 94 |
| 8.6.1: To Purchase the BACnet Support..... | 94 |
| 8.6.2: To Activate the BACnet Support..... | 95 |
| 8.6.3: Standard Object Types Supported—Life Safety Point/Life Safety Zone..... | 96 |
| 8.6.4: Standard Object Types Supported—Multi-State Input Standard Object Types..... | 97 |
| 8.6.5: Supported—Binary Output..... | 99 |
| 8.6.6: Standard Object Types Supported—Notification Class | 101 |
| Data Link Layer Options:..... | 101 |
| Device Address Binding:..... | 101 |
| Networking Options:..... | 101 |
| Character Sets Supported: | 101 |
| 8.6.7: Supported Non-BACnet Equipment/Networks..... | 101 |
| 8.7: CLSS Gateway Compatible Node Types..... | 101 |
| 8.7.1: Direct Connect Node Type Compatibility | 102 |
| Appendix A: Gateway Operating Conditions..... | 103 |
| A.1: Wirings and Power | 103 |
| Appendix B: Modulations and Power Used..... | 104 |
| Appendix C: Connecting to the Panels | 105 |
| C.1: Gateway Board Connections..... | 105 |
| C.1.1: Connecting to a Fire Alarm Panel..... | 106 |
| Improving the Signal Fidelity | 106 |
| C.2: Supported Panels..... | 107 |
| C.3: AM Series Panels | 107 |
| C.3.1: Connection Options..... | 107 |
| C.3.2: To Use an RS-232 Connection | 107 |
| C.4: ESSER Panels..... | 109 |
| C.4.1: Connection Options..... | 109 |
| C.4.2: To Use an RS-485 Connection | 109 |
| C.4.3: To Use an RS-232 Connection | 110 |
| C.4.4: Tools 8000 Settings | 112 |
| To Use an RS-485 Connection..... | 113 |
| C.4.5: Tools 8000 Settings | 115 |
| C.5: Farenhyt Panels..... | 117 |
| C.5.1: Connection Options..... | 117 |
| C.5.2: To Use an RS-485 Connection | 117 |
| C.5.3: Programming for Annunciator (ANN-PRI) | 119 |
| C.5.4: To Program for Annunciator | 119 |
| C.6: FireWarden Panels..... | 120 |
| C.6.1: Connection Options..... | 120 |
| C.6.2: To Use an RS-485 Connection | 120 |
| C.6.3: Programming for Annunciator (ANN-PRI) | 122 |

| | |
|--|------------|
| C.6.4: To Program for Annunciator | 122 |
| To Verify the Changes..... | 122 |
| C.6.5: To Use Panel's Printer Port Connection | 123 |
| C.7: Gamewell-FCI Panels | 125 |
| C.7.1: Connection Options..... | 125 |
| C.7.2: To Use Panel's Printer Port Connection | 125 |
| C.8: Gent Panels..... | 129 |
| C.8.1: Connection Options..... | 129 |
| C.8.2: Compact Series Panels..... | 129 |
| To Use a RS-232 Connection..... | 129 |
| To Use a USB Connection..... | 131 |
| C.8.3: Vigilon Series Panels | 132 |
| To Use a UART/TTL Connection | 132 |
| To Use an RS-232 Port via an I/O Card | 132 |
| To Use a USB Connection..... | 134 |
| C.9: Morley-IAS Panels..... | 135 |
| C.9.1: Connection Options..... | 135 |
| C.9.2: To Use an RS-232 Connection | 135 |
| C.10: NOTIFIER® UL..... | 137 |
| C.10.1: Connection Options..... | 137 |
| C.10.2: To Use a NUP Connection | 137 |
| C.11: NOTIFIER® European Panels (EN)..... | 141 |
| C.11.1: Connection Options..... | 141 |
| C.11.2: Preparing for Connections | 141 |
| C.11.3: To Use a NUP Connection | 141 |
| C.12: Silent Knight Panels..... | 143 |
| C.12.1: Connection Options..... | 143 |
| C.12.2: To Use an RS-485 Connection | 143 |
| C.12.3: Programming for Annunciator (ANN-PRI)..... | 145 |
| C.12.4: To Program for Annunciator | 145 |
| C.13: Triga Panels | 146 |
| C.13.1: Connection Options..... | 146 |
| C.13.2: To Use an RS-485 Connection | 146 |
| C.13.3: Programming for Annunciator (ANN-PRI)..... | 148 |
| C.13.4: To Program for Annunciator | 148 |
| C.14: VESDA® Detectors..... | 149 |
| C.14.1: Connection Options..... | 149 |
| C.14.2: To Use an Ethernet Connection | 149 |
| Before Connecting..... | 149 |
| Appendix D: Compatible Cellular Modules | 151 |
| D.1: Operation | 151 |
| D.2: Supported Modules..... | 152 |
| D.3: Standards and Codes | 152 |
| D.4: Approvals | 152 |

Section 1: General Information

1.1 About This Manual

This *CLSS Gateway Installation and Users' Manual* provides detailed procedures about installation, deployment, and upgrade of the gateway. The manual describes:

- the fixed CLSS Gateway,
- its installation environment,
- mounting and connecting the gateway circuit board to a fire detection panel, and
- initial gateway configurations

Using This Manual This manual is written with the understanding that the user is trained in the operations and services required for this product.

Usages

In this manual, product name usages are as below:

- The *CLSS Gateway* may also be referred as the *gateway*
- The *Connected Life Safety Services* mobile App may also be referred as the *CLSS App*
- The *CLSS Site Manager* may also be referred as *the Cloud*
- The term CLSS Gateway may refer to HON-CGW-MBB and CGW-MB, unless otherwise specified

1.2 Information Sources

Honeywell offers suitable information sources based on informational requirements.

1.2.1 Training Modules

Training modules are available when logged onto:

<https://fire.us.honeywell.com/#/help-videos> (For USA)

<https://fire.eu.honeywell.com/#/help-videos> (For Europe)

1.2.2 Related Documents

The table below lists documents related with the CLSS Gateway:

Table 1.1: Related Documents List

| Product Type: Honeywell Connected Life Safety Services Gateway | |
|---|--|
| For This Purpose ... | Refer to ... |
| Install quickly and operate at once | CLSS Gateway <i>Quick Installation Guide</i> P/N: 50151848-001 |
| Get comprehensive installation and configuration details | CLSS Gateway Installation and Users' Manual (This document) P/N: LS10248-000HW |
| Configure for Honeywell Alarm Transmission Service | Supplement for Honeywell Alarm Transmission Service P/N: LS10248-152HW |
| Product Type: Gent Vigilon Panels | |
| For This Purpose ... | Refer to ... |
| Install the Gent Vigilon COMPACT-24-N panels | Installation instructions Vigilon Compact panel based fire detection and alarm system Part Number 4188-1026 |
| Install the Gent Vigilon COMPACT-PLUS panels | Installation instructions Vigilon Compact Plus panel based fire detection and alarm system Part Number 4188-1101 |

Table 1.1: Related Documents List (Continued)

| | |
|--|---|
| Install the Gent Vigilon VIGPLUS-24 or VIGPLUS-72 panels | Installation instructions Vigilant Plus 4/6 Loop Control panel based fire detection and alarm system Part Number 4188-110 |
| Product Type: Notifier Panels | |
| For This Purpose ... | Refer to ... |
| NCA-2 Panel | |
| Install the NCA-2 panel | NCA-2 Installation Manual 52482 |
| NFS-320 Panel | |
| Install the NFS-320 panel | NFS-320 Installation Manual 52745LD |
| Customize the NFS-320 panel | NFS-320 Programming Manual 52746 |
| Operate the NFS-320 panel | NFS-320 Operations Manual 52747 |
| NFS2-640 Panel | |
| Install the NFS2-640 panel | NFS2-640 Installation Manual 52741LD |
| Customize the NFS2-640 panel | NFS2-640 Programming Manual 52742 |
| Operate the NFS2-640 panel | NFS2-640 Operations Manual 52743 |
| NFS2-3030 Panel | |
| Operate the NFS2-3030 panel | NFS2-3030 Operations Manual LS10006-051NF-E |
| N16 Panel | |
| Operate the N16 panel | N16 Operations Manual LS10239-051NF-E |
| Product Type: VeriFire® Tool | |
| For This Purpose ... | Refer to ... |
| Program the panels | VeriFire® Tools Help Files 51690 |
| Product Type: CLSS-Enabled LTE Commercial Fire Alarm Communicator | |
| For This Purpose ... | Refer to ... |
| Install and get started quickly | Getting Started with CLSS QHW-62051 |
| Install and operate the communicator | CLSS-Enabled LTE Commercial Fire Alarm Communicator Installation and Operating Guide LS10265-000HW-E |
| | |

Table 1.1: Related Documents List (Continued)

| Product Type: CLSS Pathway | |
|--|---|
| For This Purpose ... | Refer to ... |
| Install and wire the CLSS Pathway inside an enclosure | CLSS Pathway - <i>Product Installation Document</i> P/N: LS10338-000HW-E |
| Quickly install and configure for the central station communication | CLSS Pathway - <i>Quick Start Guide</i> P/N: LS10339-000HW-E |
| Use various installation and configuration options | CLSS Pathway - <i>Installation and Operation Manual</i> (This document) P/N: LS10340-000HW-E |
| Product Type: CLSS Connector Utility | |
| For This Purpose ... | Refer to ... |
| Install the utility and onboard the CLSS Gateway with a Central Monitoring Station | Central Station - <i>Onboarding Guide</i> P/N: LS10345-000HW-E |

1.3 Documentation Feedback

Your feedback helps us keep our documentation up-to-date and accurate. If you have any comments or suggestions about our Online Help or printed documents, you can email us.

Please include the following information:

- Product name and version number (if applicable)
- Printed document or Online Help
- Topic title (for Online Help)
- Page number (for printed document)
- A brief description of content you think should be improved or corrected
- Your suggestion for how to correct/improve documentation

Send email messages to:

FireSystem.TechPubs@Honeywell.com

Please note this email address is for documentation feedback only. If you have any technical issues, please contact Honeywell Technical Services.

1.4 Revision History

Table 1.2: Dates and Changes

| Date | Change Details |
|------------------|--|
| Rev. A | |
| October 12, 2019 | Updated for the UL normal operations support. |
| January 29, 2020 | Updated for the FCC certification support. |
| March 31, 2020 | Updated for the Intertek certification support. |
| May 01, 2020 | Updated for the IC certification support. |
| Rev. B | |
| June 22, 2020 | <ul style="list-style-type: none"> • Added the cellular modules support. • Added the <i>Upgrading the Gateway Firmware</i> section. • Updated the <i>Troubleshooting</i> section. |
| August 13, 2020 | Added the Honeywell Alarm Transmission Service section. |

Table 1.2: Dates and Changes (Continued)

| Date | Change Details |
|-------------------|--|
| October 20, 2020 | <ul style="list-style-type: none"> • Added the gateway to panel connection procedures in Appendix C. The panels are: ESSER, Gent, Morley IAS, NOTIFER UL, and NOTIFIER EN. • Updated for the NYC Fire Department certification. |
| January 07, 2021 | Added the Fire-Lite panel connection procedure in Appendix C. |
| Rev. C | |
| February 15, 2021 | Added the brand selection feature details |
| Rev. D | |
| March 08, 2021 | Revision changed for the release process. |
| Rev. E | |
| April 30, 2021 | <ul style="list-style-type: none"> • Added the Modbus connection details • Added the connection procedures for the following: <ul style="list-style-type: none"> – AM Series Panels – VESDA® Detectors – INSPIRE Panels – Fire-Lite® Panels – FireWarden Panels |
| August 15, 2021 | <ul style="list-style-type: none"> • 1.1 About This Manual: Added the <i>Usages</i> section • 1.6 Approvals: The UL details brought at the beginning • 1.6 Approvals: The FCC icon added in the FCC statement • Figure 2.1: The OC Code label added • Table 2.1: Label Name column and the OC code details added • 2.5 Security Recommendations: Added this section • Figure 3.4: Eth1 and Eth0 identified • 4.4 Honeywell CLSS Alarm Transmission Services: Updated for NOC • Appendix C: Removed the Fire-Lite connection procedure • Appendix C: Updated the FireWarden connection section with firmware details and additional notes • Figure C.2: Eth1 and Eth0 identified • C.5 FireWarden Panels: Minimum required versions details updated • C.11 VESDA® Detectors: Minimum required versions details updated |
| Rev. F | |
| January 31, 2022 | <ul style="list-style-type: none"> • Table 2.1: Usage description updated for RS-485B, RS-485A, and UART/TTL • 2.4 CLSS Gateway Parts: Added this new section • Section 3: Security Recommendation: Added this new chapter • 7.2 Functionality: Number of monitored FACP's changed to 10 • Figure 7.1: Eth1 and Eth0 are changed to Ethernet • Figure 7.2: Eth1 and Eth0 are changed to Ethernet • Figure 7.3. Eth1 and Eth0 are changed to Ethernet • 7.8 Replacing the Modbus Gateway (Modbus-GW): Added this new section |

Table 1.2: Dates and Changes (Continued)

| Date | Change Details |
|-------------------|---|
| | <ul style="list-style-type: none"> • 7.9 Using Both the CLSS Gateway and the Modbus Gateway: Added this new section • Table 7.3 CLSS-Compatible Equipment List: The Gateways column removed. The Other Products column updated. • 7.24.2 Software Configuration: Added this new section • 7.24.3 Connecting the Moxa MGate MB3180 Interface: Added this new section • C.1.1 Connecting to a Fire Alarm Panel: The Improving the Signal Fidelity section newly added • C.4 ESSER Panels: Updated for new changes • C.5 FireWarden Panels: Updated for new changes • C.6 Gamewell-FCI Panels: Updated for new changes • C.11 Triga Panels: Added this new section • C.12 VESDA® Detectors: Added this new section |
| February 07, 2022 | <ul style="list-style-type: none"> • 5.4.3 Path Selection: Dual Path selection details are added. • Section 8 The BACnet Feature: New section added. • C.12 Silent Knight section: New section added. • C.5 Farenhyt Panels section: New section added. • C.13 Triga Panels section: Supported models details updated. |

1.5 Abbreviations Used

Table 1.3: Abbreviations List

| Abbreviation | Description |
|---------------------|--|
| CLSS | Connected Life Safety Services |
| DACT | Digital Alarm Communicator Transmitter |
| ESD | Engineered Systems Distributor |
| LTE | Long-Term Evolution The wireless broadband communication standard for mobile devices and data terminals. |
| NFN | NOTI-FIRE-NET™ The network interface for NOTIFIER™ Intelligent Fire Alarm Control Panels |
| NUP | NOTIFIER Universal Protocol The Universal Protocol by NOTIFIER for all fire alarm panel communications. This protocol enables direct transfer of data between the panels and networks, without the need to translate. |
| OC | Ownership Code The code that confirms ownership of the gateway |
| POTS | Plain Old Telephone Services |
| TTL | Transistor-Transistor Logic A physical connection for performing both the logic gating and amplifying functions on the serial data. |
| UART | Universal Asynchronous Receiver/Transmitter A physical connection that converts and provides serial data for the panel and parallel data for the gateway. |
| USB | Universal Serial Bus |

1.6 Approvals

UL

S35608

FCC



FCC ID: PV3CGWMB

Compliance Statements:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including, an interference that may cause undesired operation.

Caution Statements:

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Industry Canada (IC) Statement

IC ID: 1609A-CGWMB

Compliance Statements: This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: 1) This device may not cause interference., 2) This device must accept any interference, including interference that may cause undesired operation of the device.

Déclarations de conformité: Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution Statements:

- This equipment complies with radio frequency exposure limits set forth by Industry Canada for an uncontrolled environment.
- This equipment should be installed and operated with a minimum distance of 20 cm between the device and the user or bystanders.

Déclarations de mise en garde:

- Cet équipement est conforme aux limites d'exposition aux radiofréquences définies par Industrie Canada pour un environnement non contrôlé.
- Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance du dispositif et l'utilisateur ou des tiers.

Intertek

ID: 104270338NYM-001

NFPA Compliance (USA)

Install the CLSS Gateway in accordance with the *National Fire Protection Association Installation Standard NFPA 72*.

CSFM

CSFM ID: 7300-1637:0504

FDNY

COA# 2020-TMCOAP-000121-AMND

COA# 2020-TMCOAP-000122-AMND

1.7 Warnings and Cautions in This Manual

**WARNING:**

THESE INSTRUCTIONS CONTAIN PROCEDURES TO FOLLOW TO AVOID INJURY AND DAMAGE TO EQUIPMENT. IT IS ASSUMED THAT THE USER OF THIS MANUAL HAS BEEN SUITABLY TRAINED AND IS FAMILIAR WITH THE RELEVANT REGULATIONS.



CAUTION: USERS MUST FOLLOW THE PROCESSES AND USAGES APPROVED AS PER THE REGULATORY COMPLIANCE. A CHANGED OR MODIFIED USAGE NOT EXPRESSLY APPROVED BY COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THE CLSS Gateway.

**ELECTRO-STATIC SENSITIVE DEVICES:**

TAKE SUITABLE ESD PRECAUTIONS WHEN REMOVING OR INSTALLING PRINTED CIRCUIT BOARDS.

1.8 The Product Standards



THIS GATEWAY'S PANEL IS CE MARKED TO SHOW THAT IT CONFORMS TO THE REQUIREMENTS OF THE FOLLOWING EUROPEAN COMMUNITY DIRECTIVES:

- Electro Magnetic Compatibility (EMC) Directive 2014/30/EU
- Low Voltage Directive (LVD) 2014/35/EU
- Radio Equipment Directive 2014/53/EU
- RoHS Directive 2011/65/EU
- Safety LVD Directive 2014/35/EU
- Green Directive 2011/65/EU, (EU) 2015/863
- WEEE Directive 2012/19/EU

The gateway is designed to meet Additional National Requirements: EFSG [BRE, AFNOR/CNPP, and VdS], INCERT, SBSC, EMEA, and EAC

1.9 Disclaimer

Images in the document are for reference purpose only and are subject to change. All trademarks, service marks, word marks, design marks, and logos are property of their respective owners.

Section 2: Overview

CLSS Gateway is an embedded and intelligent gateway for connected buildings. It enables system maintenance providers as well as end users to remotely manage connected fire detection systems. The gateway also supports them to ensure compliance.

2.1 Operation

The gateway acts as a portal among fire alarm panels, *CLSS Site Manager*, and peripheral devices. The gateway connection with the fire alarm panel enables reading the inventory and transmitting the data. Connection with the *CLSS Site Manager* facilitates remotely monitoring and managing the fire detection systems.

2.2 Honeywell Connected Life Safety Services

The software suite enables remote management of fire detection systems. It monitors the building's fire system events in real-time and notifies users about the events immediately. It also supports periodic maintenance activities and helps in reports generation.

2.3 Gateway Board Layout

The illustration below points out those parts that are used for connections and trouble shooting.

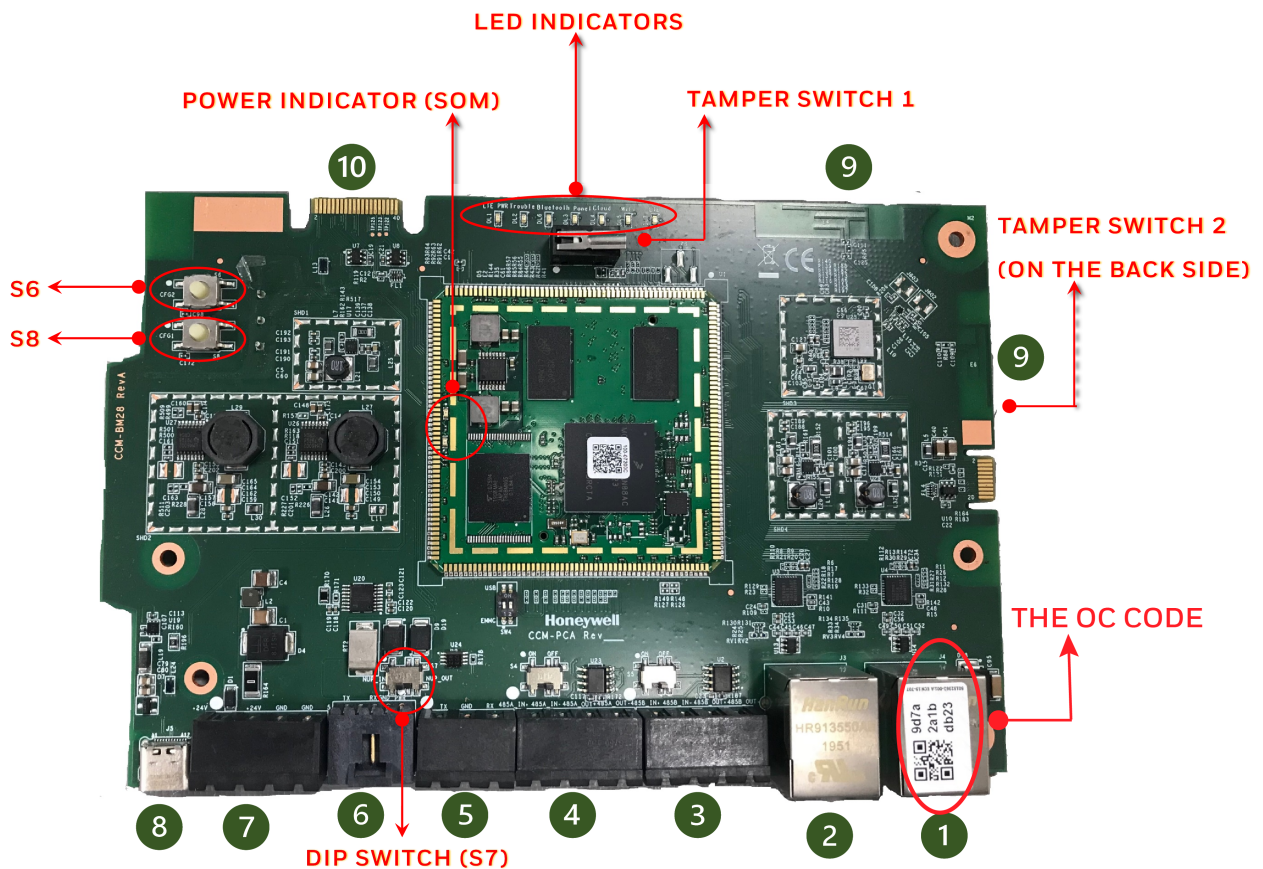


Figure 2.1: Printed Circuit Board: Layout

2.3.1 Connecting Interfaces

Figure 2.1 uses numbered labels to show the location of the interfaces for connections. This manual uses these numbered labels at various places for your convenience.

The table below uses these numbered labels to describe the type and usage of the interfaces.

Table 2.1: Gateway Interface Details

| Number in the Figure | Interface Type | Label Name | Usage |
|----------------------|-----------------|------------|---|
| 1 | Ethernet 1 | J4 | <p>Primary Ethernet port (Eth1) that can permanently connect the gateway board with the CLSS Gateway services or a Modbus client/server.</p> <p>The Ownership Code (OC) on it confirms the ownership of the board. It should be registered in the <i>CLSS Site Manager</i> during the first time installation of the CLSS Gateway.</p> <p>Cable: CAT 5 standard Ethernet cable with RJ45 connector</p> |
| 2 | Ethernet 2 | J3 | <p>Secondary Ethernet port (Eth0) providing a TCP/IP connection to a configuration computer.</p> <p>Cable: CAT 5 standard Ethernet cable with RJ45 connector</p> |
| 3 | RS-485B | P5 | Receives the alarm data and device data from an RS-485 port of a panel. |
| 4 | RS-485A | P1 | Receives the alarm data and device data from an RS-485 port of a panel. |
| 5 | UART/TTL | P4 | Receives the alarm data and device data from a UART/TTL port of a panel. |
| 6 | NUP (RS-232) | P7 | <p>Transfers fire-related and device-related data from the panel to the <i>CLSS Site Manager</i> through the gateway. It also helps in administering the fire detection system.</p> <p>Connects the gateway board to a panel's RS-232 port.</p> <p>If the connected panel supplies power, the gateway would get power from the panel through the RS-232 port.</p> |
| 7 | Power | P2 | <p>Connects to an external 24-volt DC power when required. It uses a power-limited, regulated, power-supply-listed connection for fire-protective signaling.</p> <p>Twisted-unshielded pair, 12 to 18 AWG (3.31 mm² to 0.82 mm²)</p> <p>It is used only when the gateway board is connected with:</p> <ul style="list-style-type: none"> • A network card or • When power is not supplied to the NUP connector |
| 8 | USB | J5 | For future use. |
| 9 | Wireless Aerial | E4 | Wireless antenna |
| 10 | Cellular | 4D | 40-pin connector for the compatible cellular module. |

2.3.2 LED Indicators

The LED indicators on the gateway board use different colors to identify the operational status of the gateway. To know the location of the LED indicators on the gateway board, refer to [Figure 2.1, "Printed Circuit Board: Layout"](#).

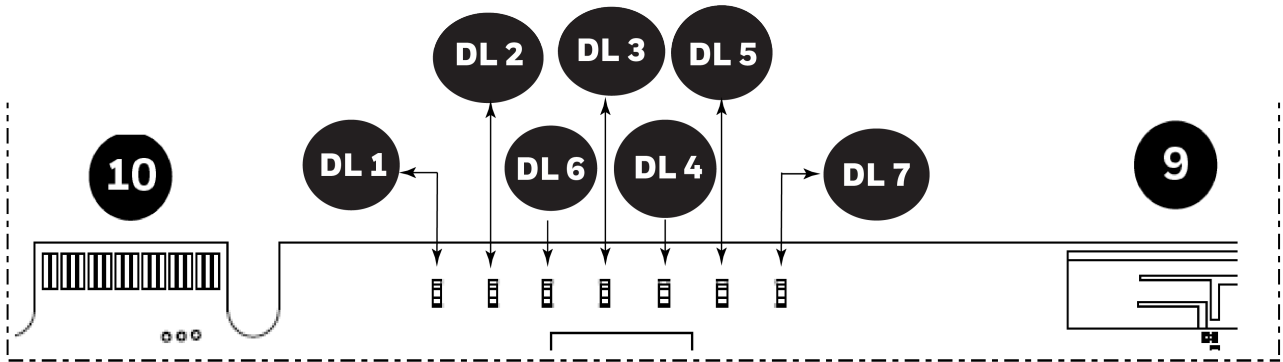


Figure 2.2: The LED Indicators on the Gateway

Table 2.2: LED Indicators and Their Messages









| | |
|---|--|
| SOM Power-Indicating LED Indicates the gateway board’s received power status. See “Power Indicator” in Figure 2.1 . | |
|  green | ON The circuit board is receiving 24V power from its power source. OFF The circuit board is <i>not</i> receiving power. |
| DL1 LTE Power LED Indicates the power supply status for cellular communications | |
|  green | ON The LTE radio device is receiving power from the circuit board. OFF The LTE radio device is <i>not</i> receiving power. |
| DL2 Trouble LED Indicates the gateway’s operational status | |
|  amber | OFF There are no issues. FLASHING SLOW (flashes once per 1 second) There are communication issues with the panel or the Internet connectivity. ON There is a critical error in the system. To fix the issues, you can refer to the 6.2, "Troubleshooting" section, which discusses about some possible issues and their solutions. |
| DL6 Mobile Connectivity LED Indicates the status of mobile communications between the gateway and the CLSS App. | |
|  Blue | FLASHING SLOW (flashes once per 1 second) The gateway is connected to the CLSS App. FLASHING FAST (flashes once per 0.25 second) The gateway is ready for the CLSS App connection. OFF The mobile connectivity is disabled. |

Table 2.2: LED Indicators and Their Messages (Continued)

| | |
|--|--|
| DL3 Panel Connectivity LED | |
| Indicates the connection status of the panel | |
|  green | FLASHING SLOW (flashes once per 1 second) The panel is connected with the gateway board. |
| | FLASHING FAST (flashes once per 0.2 second) The gateway is fetching the inventory data. |
| | ON Configuration mode is enabled for configuring the gateway network settings. |
| | OFF The gateway is <i>not</i> communicating with the panel. |
| DL4 CLSS Site Manager Connectivity LED | |
| Indicates the gateway connection status with <i>CLSS Site Manager</i> | |
|  green | ON The gateway is downloading the firmware from the <i>CLSS Site Manager</i> . |
| | FLASHING SLOW (flashes once per 1 second) The gateway is connected with <i>CLSS Site Manager</i> . |
| | FLASHING FAST (flashes once per 0.2 second) The gateway is connected with Internet, but not connected with the <i>CLSS Site Manager</i> . |
| | OFF The gateway is <i>not</i> connected with Internet. |
| DL5 Wireless Connectivity LED | |
| Indicates the gateway wireless connectivity status | |
|  green | FLASHING SLOW (flashes once per 1 second) The wireless connectivity is enabled for the <i>CLSS Site Manager</i> connection. |
| | OFF The wireless connectivity is disabled. |
| DL7 Cellular Connectivity LED | |
| Indicates the LTE radio connection status | |
|  green | FLASHING SLOW (flashes once per 1 second) The LTE radio is transmitting data. |
| | FLASHING FAST (flashes once per 0.2 second) The LTE radio may have a connectivity issue, which requires attention. |
| | OFF There is no cellular connection. |

2.3.3 Switches on the Gateway Board

Below table informs about the switches on the gateway board. To locate the switches on the gateway board, refer to [Figure 2.1: "Printed Circuit Board: Layout"](#).

Table 2.3: Gateway Board Switches

| Switches | Purpose |
|-----------------|---|
| S6 | For securely configuring the gateway's settings Pressing the switch for six seconds switches the gateway board to the configuration mode. |
| S7 | For changing the direction of the 24V power of the NUP/RS-232 connector NUP_IN: The gateway board receives power through its NUP/RS-232 port. NUP_OUT: The gateway board receives power through its power supply port, which is connected to an external power supply source. |
| S8 | For enabling mobile pairing Pressing the switch for ten seconds enables mobile pairing. |
| Tamper Switches | Purpose |
| Tamper 1 | For alerting whenever the gateway enclosure door is opened It is located at the front-side of the gateway, next to the LED indicators. |
| Tamper 2 | For alerting whenever the gateway board is removed from the enclosure It is located at the backside of the gateway. |

2.4 CLSS Gateway Parts

| Part Number | Description |
|--------------|--|
| HON-CGW-MBB | CLSS Gateway with enclosure |
| CGW-MB | CLSS Gateway board |
| CGW-BB | CLSS Gateway enclosure |
| 50160636-001 | CLSS Gateway kit. It includes a 30" NUP cable and a NOTIFIER lock and key set. |
| 32351718-001 | 10 ft NUP Serial (RS-232) cable kit |

Section 3: Security Recommendations

3.1 For Users

An administrator should:

- Regularly review the user roles and permissions for a CLSS account
- Immediately remove users who should no longer have access to CLSS

A technician should:

- Use discretion to allow or deny a location access request.
- Disconnect the *CLSS App* from the *CLSS Gateway*, once the required activity is completed.
- Turn OFF the location access in the CLSS App's **Security Settings**, when location access is not required.

3.2 For Preventing Potential Risks

Security threats applicable to networked systems include unauthorized access, communication snooping, viruses, and other malicious software agents.

3.2.1 Unauthorized Access

Unauthorized access results from unsecured user name and password, uncontrolled access to the equipment, or uncontrolled and unsecured access to the network.

It results the following:

- Loss of system availability
- Incorrect execution of controls causing damage to the equipment
- Incorrect operation, spurious alarms, or both
- Theft or damage to the contents of the system
- Capture and modification or deletion of data causing possible liability to the installation Site and Honeywell

User Access and Passwords

Observe the following good practices:

- The password has one numerical, one upper case, one lower case, and one special character whenever any user registers or changes the credentials.
- Enforce a password change periodically
- Do not allow any dictionary words as passwords
- Check passwords against known common weak password databases
- Do not allow common and predictable passwords though they meet other requirements. For example: P@SSwOrd
- Not allow usernames, service names, or any such context-specific words
- Passwords should be complex and not easily guessed; and, should not contain phrases used in common speech.
- Do not use personally identifiable information as a password, such as social security numbers, addresses, birth dates.
- Provide only the minimum level of access and privileges for each user.
- Ensure physical security of passwords. Avoid and warn against writing user names and passwords where they can be seen by unauthorized personnel.
- Periodically audit user accounts and remove any that are no longer required.

3.2.2 Memory Media

- Use only authorized removable media.
- Use an up-to-date anti-virus software to scan the removable media and check for viruses and malware.
- Ensure that the memory media is not used for other purposes to avoid risk of infection.
- Control access to media containing backups to avoid risk of tampering.

3.2.3 Software and Firmware Updates

System software and firmware updates may be offered from time to time.

Ensure that your local representative:

- Has the up-to-date contact details, and
- Periodically visits the Honeywell web site for up-to-date product information

3.2.4 Viruses and Other Malicious Software Agents

Malicious Software include the following:

- Viruses
- Spyware
- Worms
- Trojans

These may be present in a computer using a Monitoring Station Software or in a USB pen drive, which is used to copy data to computer.

The intrusion of malicious software agents can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data — including configuration and device logs.

USB devices from other infected systems on the network or malicious Internet sites can also transfer viruses.

3.2.5 Network and Firewall Setup

Inbound (In) Port: The port another computer uses to access a gateway functionality. An application on the gateway will be actively listening on this port for client connections.

Outbound (Out) Port: The gateway uses outbound ports to connect to Internet or *CLSS Site Manager*. The Cloud services in the *CLSS Site Manager* will be listening on these ports waiting for a connection from the gateway.

By default, block all inbound and outbound connections and allow only the ports listed in the below table:

| Port Number | Type | IN/OUT | Purpose/Remarks |
|-------------|-------------|---------------|--|
| 443 | HTTPS - TCP | Bidirectional | NOC APIs communications with a Supplier Cloud and <i>CLSS Site Manager</i> |
| 1433 | TCP | Bidirectional | NOC Server and SQL DB private network-based communications |
| 9000 | TCP | Bidirectional | Pathway devices and NOC communications |
| 9000 | UDP | Bidirectional | Pathway devices and NOC heartbeat communications |
| 6000 - 6030 | TCP | Bidirectional | Monitoring station and NOC communications |

The *CLSS Pathway* device sends alarms to *CLSS Site Manager*, using the below endpoints:

| Region | All End-points |
|---------|--|
| West US | <ul style="list-style-type: none"> • https://fireclssnocwus.honeywell.com/clssnocalarmrcvr/ • https://fireclssnocwus.honeywell.com/clssnocapisrv/ |
| East US | <ul style="list-style-type: none"> • https://fireclssnoceus.honeywell.com/clssnocalarmrcvr/ • https://fireclssnoceus.honeywell.com/clssnocapisrv/ |

Best Practices: Network Security

Open protocols, unencrypted connections, and unauthenticated sites are risks.

Ensure the following:

- Required firewalls and VPN connections are in place
- The logging systems monitor malicious activity and perform regular audits
- Unused services and ports are disabled
- Security patches are up to date
- Users have only minimum required privileges for files and folders

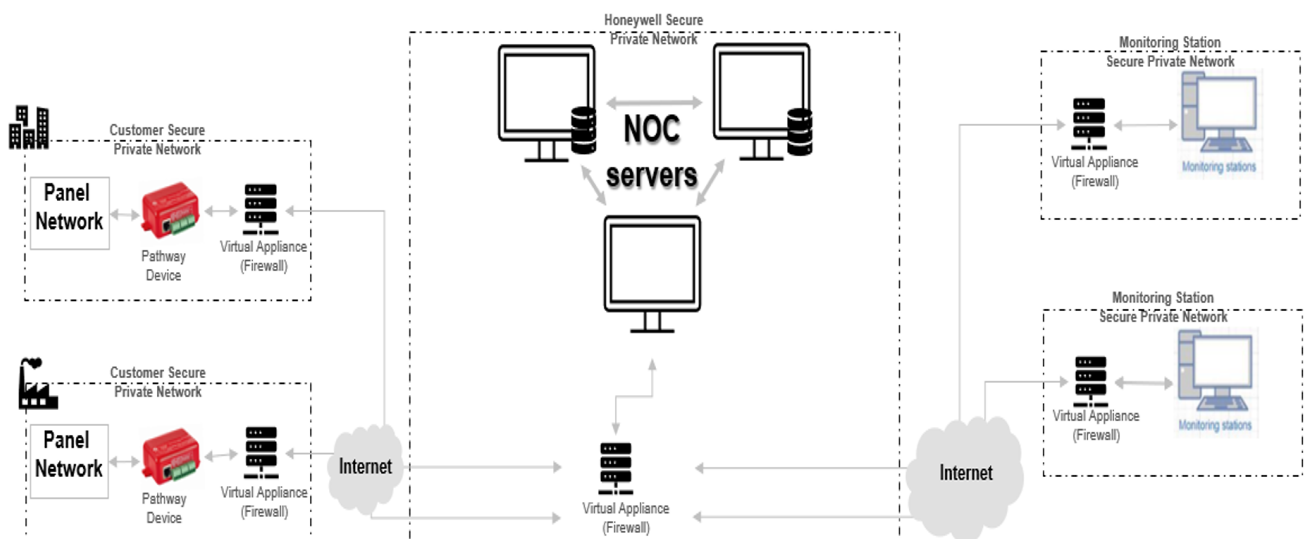
Best Practices: Connected Devices

■ For VESDA Detectors

- Adhere to the xtralis security guidelines: <https://xtralis.com/file/9584>
- When connected with one VESDA detector, use a short point-to-point link between the VESDA detector and the CLSS Gateway.
- When connected with multiple VESDA detectors, allow only the VESDA detectors and the gateway connections. Do not allow any other connections.
- Allow only authorized personnel to configure VESDA devices.

3.2.6 Securing the Monitoring Stations

- Good security practices should be observed on the Monitoring Station PCs.
- Operating systems and software should be kept up to date by installing the manufacturers updates, as well as maintaining up-to-date anti-virus software on all computers, which may be connected directly or via a network.
- For monitoring stations, it is recommended to use secure VPN channel, which must be placed behind the firewall.
- It is suggested to use hardware receiver as an adapter at the monitoring station.
- For the CLSS Pathway devices, it is recommended to use secure private network, and keep them behind the firewall.
- Only authorized personnel should get access to private network.
- Best industry standards should be followed while configuring the firewall policies.
- Devices should be safely installed in the secure zone and they must be out of reach to unauthorized personnel.
- Ensure that the computers are regularly scanned for viruses.
- Only install files and software from trusted sources and use only them on associated computers to avoid malicious software.
- Use only authorized removable media. For example, use CD, DVD, external hard drives, or USB memory sticks, which have been scanned using up-to-date anti-virus software.



Section 4: Installation

You can use a fixed gateway in the fire detection system.



NOTE: This section refers to the fixed gateway P/N: HON-CGW-MBB. For instructions on mounting the portable gateway, P/N: CGW-MB, refer to the NBB-2 installation document LS10250-000NF-E.



CAUTION: THE GATEWAY MUST BE INSTALLED INDOORS IN A DRY LOCATION.



WARNING: INSTALL AS PER THE LOCAL BUILDING AS WELL AS CUSTOMER-SPECIFIC REQUIREMENTS. FOR EXAMPLE, INSTALLING AND OPERATING THE GATEWAY WITH ITS WIRELESS TECHNOLOGY MIGHT BE RESTRICTED NEAR MEDICAL EQUIPMENT, FUELS, OR CHEMICALS. ENSURE THAT THERE ARE NO CONFLICTS.

4.1 Wall Mounting the Fixed Gateway

It is recommended to keep the gateway within 1 meter (3-feet) from the connected panel or the network card. The minimum distance between the gateway and the panel should be 30 cm.



CAUTION: THE EQUIPMENT IS SUITABLE FOR MOUNTING AT A MAXIMUM HEIGHT OF 9.9 FEET ONLY.



NOTE: In a low LTE signal area, you may choose to use external aerials.

Follow the instructions below to mount the gateway enclosure:

1. Open the package and take out the contents.
2. Inspect the contents for damage. If there is any damage, do not proceed with installation. Return the package.
3. Place the right-side door edge on a flat surface for support.
4. At the right-side door edge, punch out a hole for the door locking screw or for an optional keyed lock (see [Figure 4.1](#)).

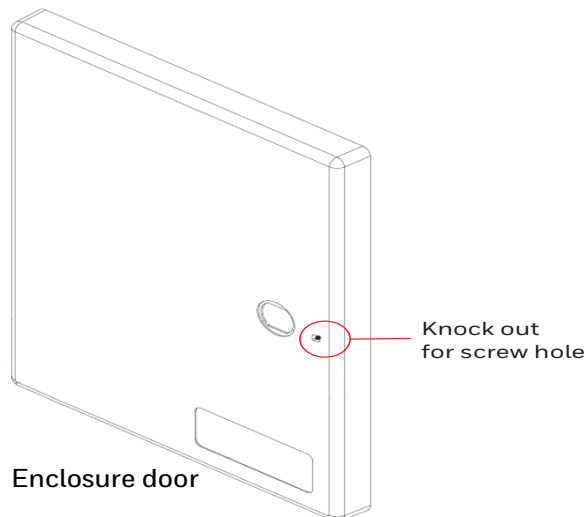


Figure 4.1: Screw Hole Knock Out

5. Depending upon the wall construction, select suitable screws to mount the enclosure.
6. Place the backbox on the wall where the enclosure is to be mounted.
7. Confirm that the placement of the backbox allows the door to swing open freely.

8. Mark and pre-drill the hole for the top mounting bolt (see [Figure 4.2](#)).

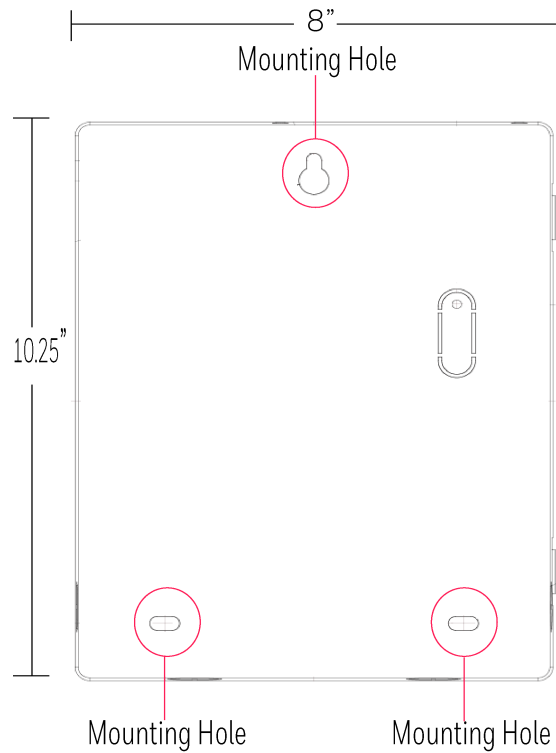


Figure 4.2: Mounting the Backbox

9. Remove the backbox.
10. In the top mounting hole, insert the mounting screw.
11. Tighten the screw, leaving space for hanging the enclosure.
12. Mount the backbox over the top screw and level it.
13. Mark the locations for the two lower mounting holes.
14. Remove the backbox and drill the mounting holes.
15. Mount the backbox over the top screw, then install the remaining fasteners.
16. Tighten all fasteners securely.

4.2 Mounting the Portable Gateway

Section reserved for future functionality.

4.2.1 Mounting onto the Chassis

Section reserved for future functionality.

4.3 Gateway Board Connection Options

The gateway board can be connected with a cellular module, wireless aerials, the CLSS Site Manager, a configuration computer, a panel, a mobile device, and an external power supply.

Figure 4.3 illustrates the connection options at the top side of the gateway board.

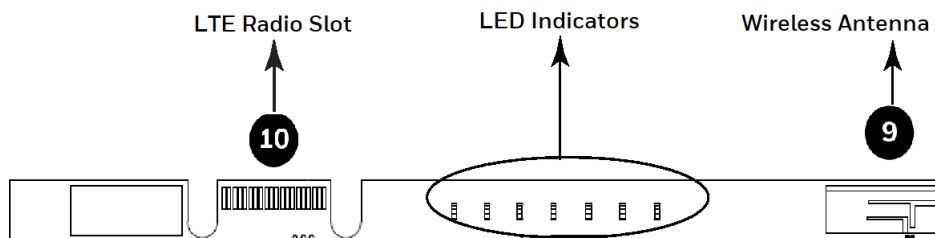


Figure 4.3: Gateway Connections - Top Side

Figure 4.4 illustrates the gateway connection options at the bottom side of the gateway board.

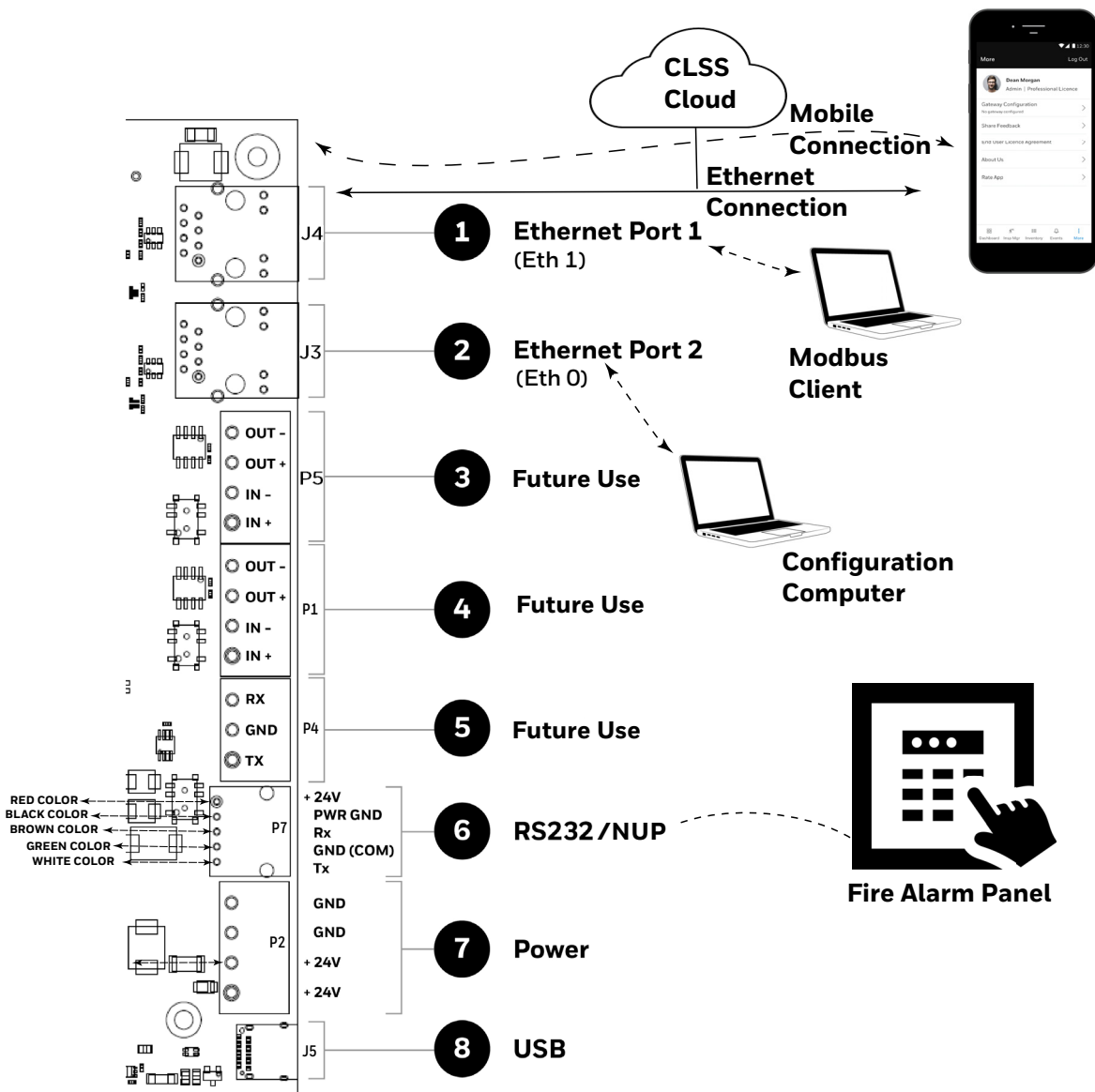


Figure 4.4: Gateway Connection Options - Bottom Side

4.3.1 Connecting to a Fire Alarm Panel

To know about supported panel variants, their connection options, and commissioning procedure, refer to the [“Connecting to the Panels” on page 105](#).

4.3.2 Installing a Cellular Module

Cellular modules enable value-added alarm transmission services from a protected premises to the CLSS-connected site and to a central receiving station. If required, you can plug in the device onto the gateway board.



NOTE: When the gateway is communicating to a central station through cellular connection, it uses the primary Ethernet connection for *CLSS Site Manager* communications.

Compatibility Requirements

To ensure proper operation, these cellular module shall be compatible with the CLSS Gateway.

To know more about the supported devices, refer to [“Compatible Cellular Modules” on page 151](#).

Before Installing a Cellular Module

- If installing on an existing operational gateway, inform the operator and local authority that the gateway will be temporarily out of service.
- Disconnect power to the gateway.

Precautions for Service Quality

- Carefully select the installation location of the CLSS Gateway.
- Do not mount the gateway on or near metal objects. This includes steel cabinets, metal walls, steel beams, steel roofs or roofing girders, foil backed insulated walls, and duct works.
- During the installation, periodically monitor the signal quality via the CLSS App to predict QoS (Quality of Service) of the LTE radio over time.

If the installation location does not offer good QoS, try the following options:

1. Move the gateway to achieve the best QoS. Typically, moving it to a higher placement offers the best QoS.
2. Use an optional antenna external aerial connection. Antenna must be located in the same room as the CLSS Gateway enclosure. Refer to the [See “To Install an External Antenna” on page 28](#) for details.

To Install a Cellular Module

The installation involves plugging the cellular module onto the gateway board, and securing the mounted device with a retention strap. The strap will compress the RF ground system between the cellular modules and the gateway board assembly.

1. Switch OFF the gateway.
2. Punch out the appropriate knockouts on the enclosure for the aerials (see [Figure 4.5](#)).

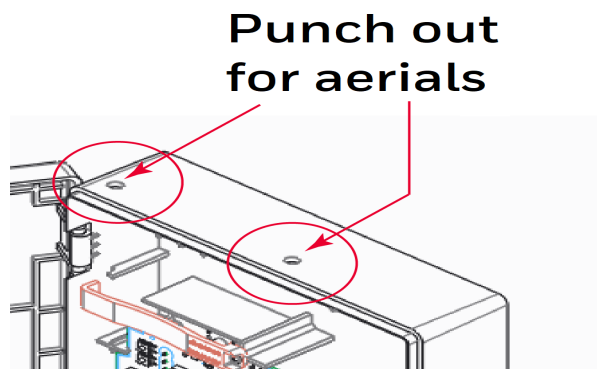


Figure 4.5: Knockouts on the Enclosure

3. Open the enclosure door.
4. On the top edge of the gateway, plug the cellular module onto the 40-pin expansion slot (see [Figure 4.6](#)).



WARNING: DO NOT USE THE SCREW ON THE TOP EDGE OF THE CELLULAR MODULE. IT WILL ADVERSELY AFFECT THE RADIO PERFORMANCE. REFER TO THE DO NOT USE THIS SCREW SHOWN IN THE FIGURE 3.4.

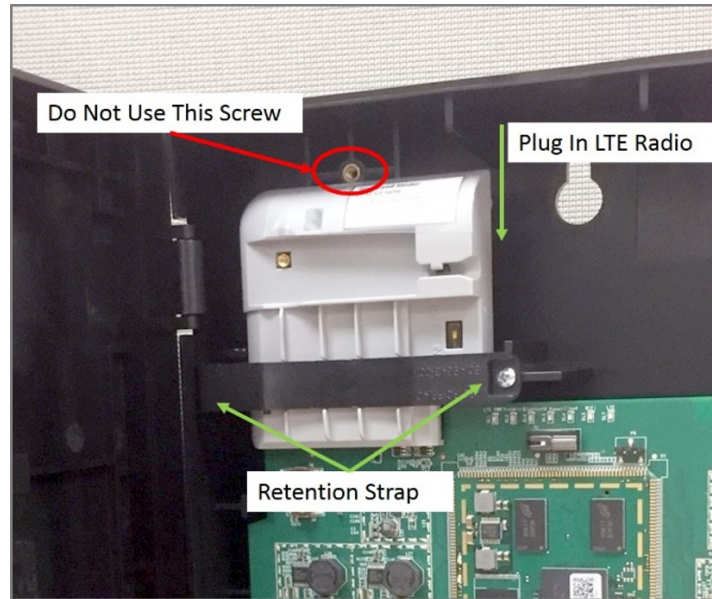


Figure 4.6: Installing the Cellular Module

5. Secure the cellular module with the retention strap and a screw, which come with the module (see [Figure 4.6](#)).



WARNING: FAILURE TO USE THE RETENTION STRAP MAY ADVERSELY AFFECT THE AERIAL PERFORMANCE.

Replacing the SIM Card

The cellular module comes with a factory-mounted SIM card. If necessary, replace it as follows:

1. Open the gateway door.
2. Remove the NUP cable or the 24v DC power cable to switch OFF the gateway board.
3. Remove the retention strap screw and the retention strap (see [Figure 4.6](#)).
4. Slide the cellular module upward to disconnect it from the gateway board.
5. Carefully remove the back cover of the cellular module.

- Find the SIM card holder and slide its door to unlock (see [Figure 4.7](#)).

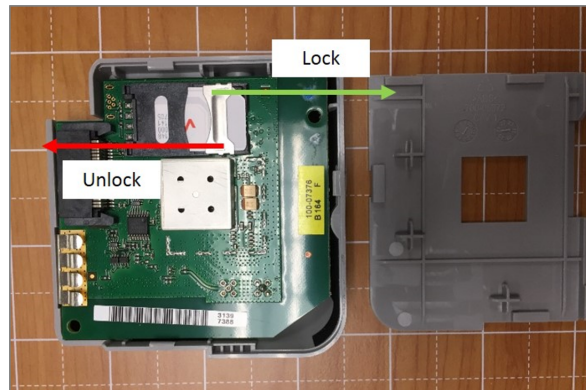


Figure 4.7: Unlock or Lock Movement

- Remove the old SIM card and replace it with the new card.
- Slide the card holder door back and lock it (see [Figure 4.7](#)).
- Place the bottom cover onto the communicator and snap it closed.

4.3.3 Installing the External Aerials

In a low LTE signal area, using an external aerial may boost the signals. When installing an aerial, ensure that:

- The aerial is within its granted FCC directional gain limitations
- The installation is in accordance with the manufacturer's instructions

To Install an External Antenna

- Switch the SW1 switch on the cellular module to EXT.
 - Connect the internal coax adapter onto the module.
 - Route the coax adapter cable through the knock out on the enclosure.
 - Tighten the nuts at both sides of the knock out.
 - Take the external antenna.
 - Thread the antenna onto the antenna connector and tighten it.
 - (If there is a magnet at the bottom of the antenna) Attach the magnet onto the top wall of the enclosure.
- Or
(Optional) Use a double-sided adhesive tape to secure the attachment.

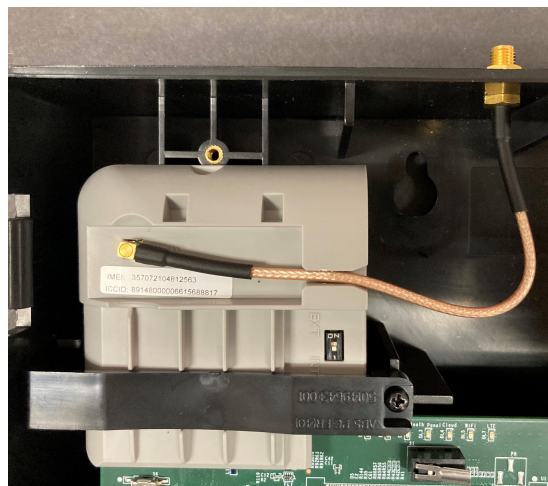


Figure 4.8: Installing an External Antenna

Section 5: Configurations

The gateway settings control the gateway's communications with the mobile, panel, detectors, and *CLSS Site Manager*.

5.1 Commissioning the Gateway

You can commission the CLSS Gateway for an already added customer or for a new customer.

5.1.1 The Commissioning Steps

Step 1: Connect to the IP network through the Ethernet 1 port of the gateway for the *CLSS Site Manager*.

Step 2: Send the panel's topology onto the *CLSS Site Manager*.

Refer to the [Exporting Panel's Topology Data](#) section.

Step 3: Connect the gateway to a panel.

Refer to the [Connecting to the Panels](#) section.

Step 3: Configure the gateway to use the connected panel.

Refer to the [Configurations](#) section. (The current section)

Steps 4: Inspection and maintenance of the gateway.

5.1.2 Exporting Panel's Topology Data

The first-time commissioning of the gateway includes uploading the panel's topology data to the *CLSS Site Manager*.



NOTE: The topology data is exported using the supported panel manufacturer's programming tool. To know about their recommended tool for exporting and related configurations, refer to the panel's documentation.

To Export the Topology Data

1. Using the tool, which the panel manufacturer recommends, export the panel's topology data into your configuration computer.
2. From the configuration computer, log into the *Connected Life Safety Services* application.
3. Ensure that the relevant *customer*, *site*, and *building* details are available in the application.
4. Select the building where the panel is located.
5. Go to the building's inventory page.
6. Click on the **Config File** button, find the exported topology data file, and select that file.
7. Wait for the upload success message.
8. Confirm that the inventory page shows details of the panel's connected devices.

5.1.3 To Configure via the Wireless Connection

1. In the mobile device, download the *Connected Life Safety Services* App from Play Store or App Store.
2. Install the App.
3. From the Honeywell on-boarding email, note down the login credentials.
4. On the mobile device, log into the *CLSS* App.
5. On the App's dashboard, at the right bottom, tap the **More** icon (see [Figure 5.1](#)).

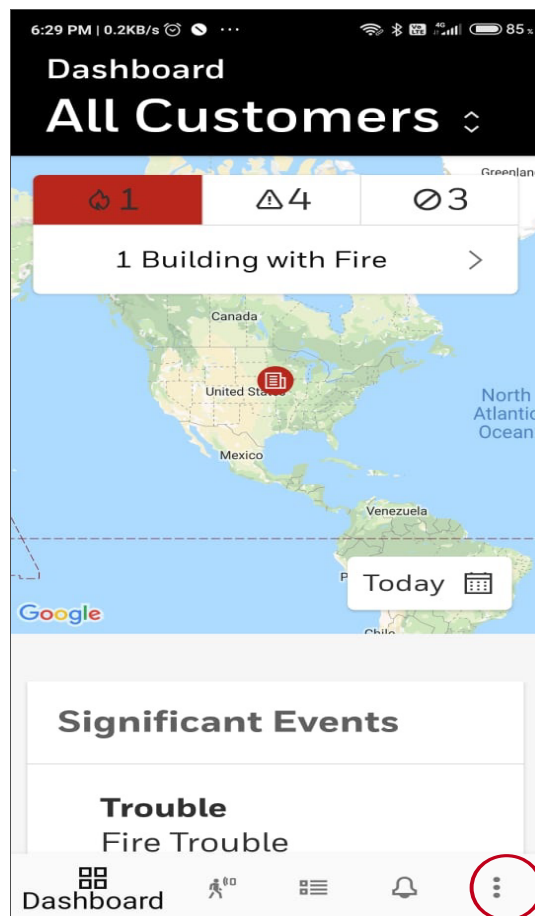


Figure 5.1: CLSS App Dashboard

6. Tap **Gateway Configuration**.
7. Follow the on-screen instructions for mobile connectivity.



NOTE: Based on the gateway you are configuring, select either *Portable Gateway* or *Fixed Gateway*.

8. Wait for the App to connect with the gateway, the fire alarm panel, Internet, and *CLSS Site Manager*. The App notifies you when configuration is completed.
9. On the dashboard, from the **All Customers** option, find the required *customer > site*.
10. Tap on the specific building.
11. To commission the gateway, tap on **CONNECT GATEWAY** and follow the on-screen instructions (see [Figure 5.2](#)).

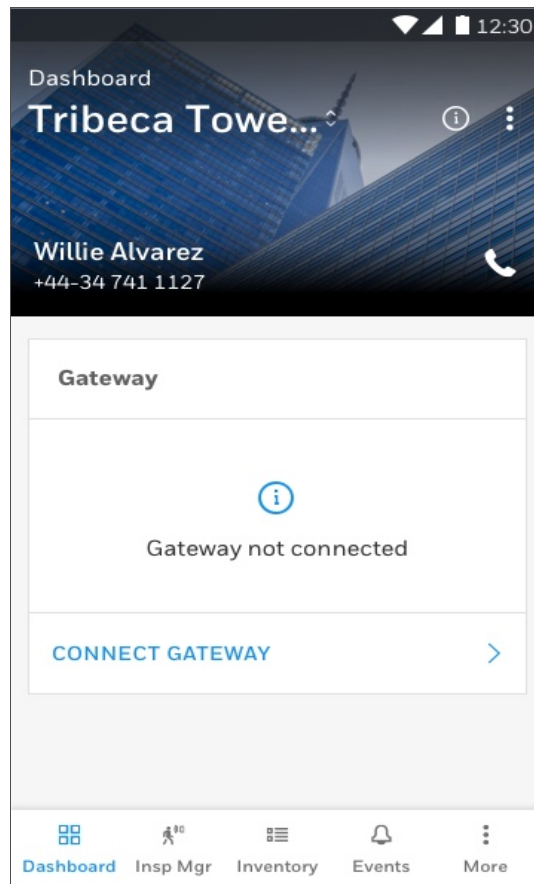


Figure 5.2: Building Details Page



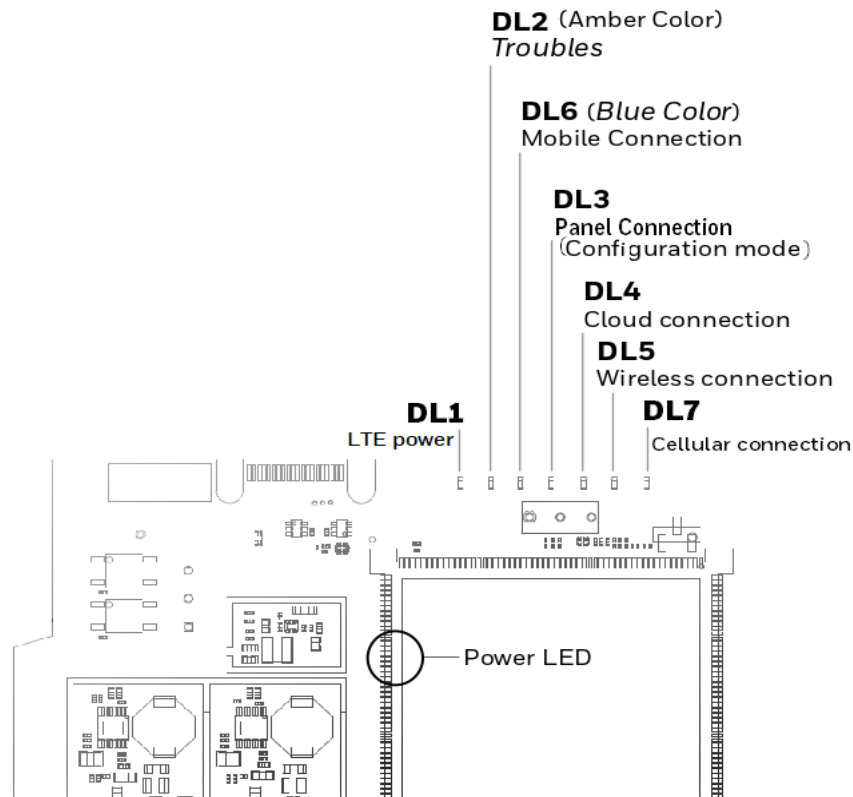
NOTE: In the *Connected Life Safety Services App*, the option to enable the control functionality is available for 60 minutes, which can be extended.

At the end of 60 minutes, the user will have the option to extend the session. If not extended, the session will expire after 60 minutes and the user must enable a new session of control functionality within the *Connected Life Safety Services App*.

5.2 Verifying the Gateway Connections

While configuring the gateway, confirm that the LEDs indicate successful connections as shown in [Figure 5.3](#).

If the LED is indicating differently, refer to [Table 2.2](#) to know the operational status. If necessary, refer to the [6.2, "Troubleshooting"](#) section to fix the problem or contact Honeywell Technical Support.



| LED Indicator | State | Meaning |
|----------------------|----------------------------|--|
| Power-Indicating LED | ON | Successful power connection |
| DL1 | ON | ON - The cellular module is installed and receiving power. |
| | OFF | OFF - The cellular module is not installed. |
| DL2 | OFF | There are no issues |
| DL6 | Flashing fast ^a | Successful mobile connection |
| | Flashing slow ^b | Ready for connection |
| | OFF | Disabled mobile connection |
| DL3 | ON | The gateway is in the configuration mode |
| | Flashing fast | The gateway is getting the inventory data |
| | Flashing slow | The gateway is communicating with the panel |
| DL4 | Flashing slow | The gateway is communicating with <i>CLSS Site Manager</i> |
| | Flashing fast | The gateway has the Internet connectivity, but not the <i>CLSS Site Manager</i> connectivity |

a FLASHING FAST = 0.2 second ON and 0.2 second OFF

b FLASHING SLOW = 1 second ON and 1 second OFF

| LED Indicator | State | Meaning |
|---------------|---------------|---|
| DL5 | Flashing slow | The gateway has wireless connection with <i>CLSS Site Manager</i> |
| DL7 | OFF | There is no cellular connection. |
| | Flashing slow | The LTE radio is transmitting data for the cellular connection. |
| | Flashing fast | The LTE radio has connectivity issues. |

Figure 5.3: Connection Indicators

5.3 Panel Brand and Connection Settings

When the mobile App is connected with the *CLSS Site Manager*, you can change the panel brand's communication settings.



NOTE: You can change the connection settings using either the CLSS mobile App or the *Gateway Configuration Tool*.

5.3.1 To Change the Connection Settings

1. To change the newly connected panel's settings:
 1. Select the Customer and the Site.
 2. Tap on your connected gateway from the list of gateways.

OR

To change the previously connected panel's settings:

 1. Tap the three dots at the top right on the mobile App.
 2. Tap **Install Fixed Gateway**.
 3. Select the Customer and the Site.
 4. Tap on your connected gateway from the list of gateways.
2. Tap on the **Panel Brand & Connection** option on the **Gateway Summary** screen.
3. Tap on **Panel Brand**.
4. Change the panel brand, if required.
5. Tap **NEXT**.
6. Select the connection type for the panel from the **Connection Type** screen.
7. Tap **APPLY**.
8. Tap **Panel Type** on the **Gateway Summary** screen.
9. Change the values for the panel brand on the **Communication Settings** screen.
10. Tap **SAVE**.

5.4 Honeywell CLSS Alarm Transmission Services

The CLSS Gateway enables the central monitoring service providers, fire department, and its building occupants to have the quickest response possible to an event. The building occupants are given early, personalized guidance to safety.

This service also increases the first-time fix rate for all service providers. Its predictions about certain upcoming needs reduce business disruptions as well.



NOTE: This special service is available only to select service providers. For more details, contact Honeywell Technical Support.

Communication Management

- The communication path between the gateway and the Central Station is supervised. The default supervision timing is 5 minutes.
- In case of an AC failure, the CLSS Gateway communicates to the central station after 120-minutes.

5.4.1 Central Station Communication

The CLSS Gateway receives events from a listed Fire Alarm Control Unit and transmits events using cellular, wireless, or Ethernet to Honeywell's Network Operations Center (NOC). All signals from the CLSS Gateway are delivered to Honeywell's NOC, which routes the events to the appropriate central monitoring station over telephone networks, IP networks, or both.

5.4.2 Activating the Central Station Communication

In the *CLSS Site Manager*, the service provider administrator should activate the central station communication. It is a one-time activity, which can be done for an operational gateway or for a newly installed gateway.



NOTE: Before activating the central station communication, ensure that the CLSS Gateway has no communication failures. During a connection failure, the CLSS Gateway cannot send event data to the *CLSS Site Manager* or the NOC. For example, if the gateway's Ethernet cable is disconnected, its fire panel will display *UDACT Trouble*. Only after restoring the connection and clearing the trouble, the *CLSS Site Manager* or the NOC can receive events again.

Adding a Central Station to the CLSS Account

Only those central stations added in the external accounts of the *CLSS Site Manager* can receive alarms the gateway sends. Therefore, a service provider administrator should first perform this one-time activity and add the accounts.



NOTE: Using the credentials given, you can log onto the *CLSS Site Manager* available on <https://fire.honeywell.com> and enable this feature. Honeywell recommends Chrome browser for using the *CLSS Site Manager*.

1. Log onto the *CLSS Site Manager*.
2. Click on the profile icon at the top right and click **External Accounts**.
3. Click **ADD NEW** under the **Central Stations** section.
4. Follow the on-screen instructions to add the central station account.

Install a Fixed Gateway at the Site

To enable central station communications, a CLSS Gateway must be installed.



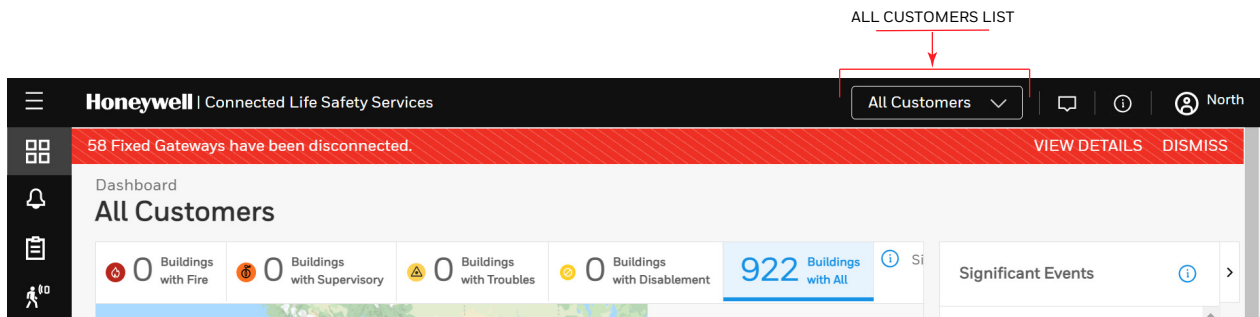
NOTE: You can skip this procedure if you are activating the central station communication for a CLSS Gateway that is already installed.

1. Log into the *Connected Life Safety Services App* in your mobile device.
2. Tap the three horizontal dots icon at the top-right side on the **All Customers** dashboard.
3. Select **Install Fixed Gateway** from the pop-up menu.
4. Follow the on-screen instructions to complete the gateway installation in the App.

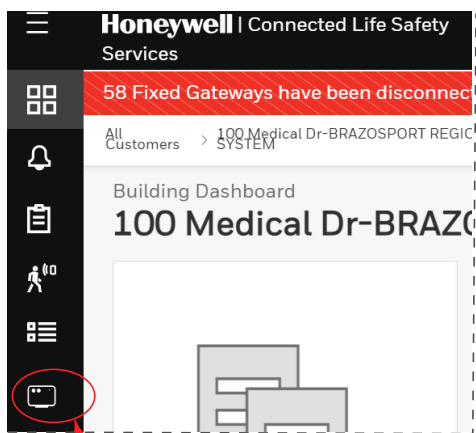
Configuring the Central Station Communication

A technician or a service provider administrator can configure the central station communication of the CLSS Gateway.

1. Log onto the CLSS Site Manager.
2. Select the customer from the **All Customers** list at the top-left side.



3. Select the customer, select the site, and then select the building requiring alarm transmission.
4. Click the **FEATURE ACTIVATION** icon at the left navigation bar.



THE FEATURE ACTIVATION ICON

5. Select **Installed Gateways** and then go to the **INSTALLED GATEWAYS** section.



NOTE: To view only those gateways not yet activated, select **Show only Gateways without activations** at the right side.

6. Find the CLSS Gateway requiring alarm transmission from the gateway list shown.

7. Click on the specific CLSS Gateway of the building.
8. Click on the **Connected Gateway** activation card inside the selected gateway.
9. Click **Configure Now**.
10. Select the central station to configure from the central stations list.
11. Follow the on-screen instructions to enable the alarm transmissions.

Verifying the Central Station Communication Configurations

After configuring for the central station communication, call the central station to confirm that the alarm transmission for the building is activated.

5.4.3 Dual Path Communication for Alarm Transmission

While configuring the central station communication, you can choose a single path or two paths for alarm transmissions. Reporting options are: LTE cellular only, IP only, IP Primary with LTE cellular backup, or LTE Cellular Primary with IP backup.



NOTE: Alarms will be sent through two among the following ports: Ethernet, Wireless, or Cellular.

Supervision Period

Dual paths are monitored for integrity at an interval period as per NFPA 72 requirements. In case of a failure, both the local premises and the central station receive a failure report with a unique code as in the central station report.

Transmission Options

| Path Options | Available Paths | Supervision Interval |
|--------------------|-----------------|----------------------|
| Single Path | | |
| Cellular | 2010 Cell | 5 Minutes |
| | 2013 Cell | 60 Minutes |
| IP | 2010 IP | 5 Minutes |
| | 2013 IP | 60 Minutes |
| Dual Path | | |
| IP and Cellular | 2010 IP & Cell | 24 Hours |
| | 2013 IP & Cell | 6 Hours |

Section 6: Post-Installation Activities

The system maintenance provider is responsible for the maintenance and upkeep of the CLSS Gateway. The maintenance involves avoiding potential issues, making regular backups, restoring data when required, collecting data for troubleshooting, and other activities.

6.1 Upgrading the Gateway Firmware

CLSS Service Manager notifies the gateway administrators when a new firmware is launched. The administrators can perform the upgrade at a planned time.



CAUTION: BEFORE UPGRADING ENSURE TO GET PERMISSION FROM THE SITE. THE REBOOT AFTER THE UPGRADE SHOULD BE AT A MUTUALLY PLANNED TIME WITHOUT AFFECTING THE OPERATION.

The upgrade happens in the background while the system is running. After the upgrade the gateway will reboot.



CAUTION: PREVENT ANY DISTURBANCE TO THE POWER CABLE OF THE GATEWAY DURING THE UPGRADE.

6.1.1 To Upgrade Before Commissioning the Gateway

1. Connect the gateway to Internet.



NOTE:

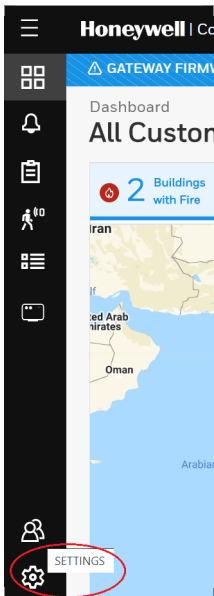
- The Internet connection can be either wireless or LAN.
- The LED indicator DL4 on the gateway flashing Green confirms Internet connection.

2. Log onto the *CLSS Site Manager*.
3. Click **VIEW** on the notification at the top.



Or

Click the **SETTINGS** icon at the bottom left.



4. Click **Gateway Management** in the **Settings** page.
5. Click **Add Gateway** on top.

6. Enter the OC of the gateway in the **Add Gateway** dialog and click **ADD**.
7. Wait for the registration to complete.
8. Enter the OC of the gateway in the **Search OC** field to find the gateway to update.

Or

Scroll across to find the gateways to update.

9. Click **Update**.

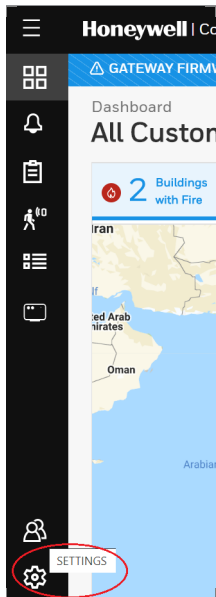
6.1.2 To Upgrade After Commissioning the Gateway

1. Log onto the *CLSS Site Manager*.
2. Click **VIEW** on the notification at the top.



Or

Click the **SETTINGS** icon at the bottom left.



3. Click **Gateway Management** in the **Settings** page.
4. Enter the OC of the gateway in the **Search OC** field to find the gateway to update.

Or

Scroll across to find the gateways to update.

5. Click **Update**.

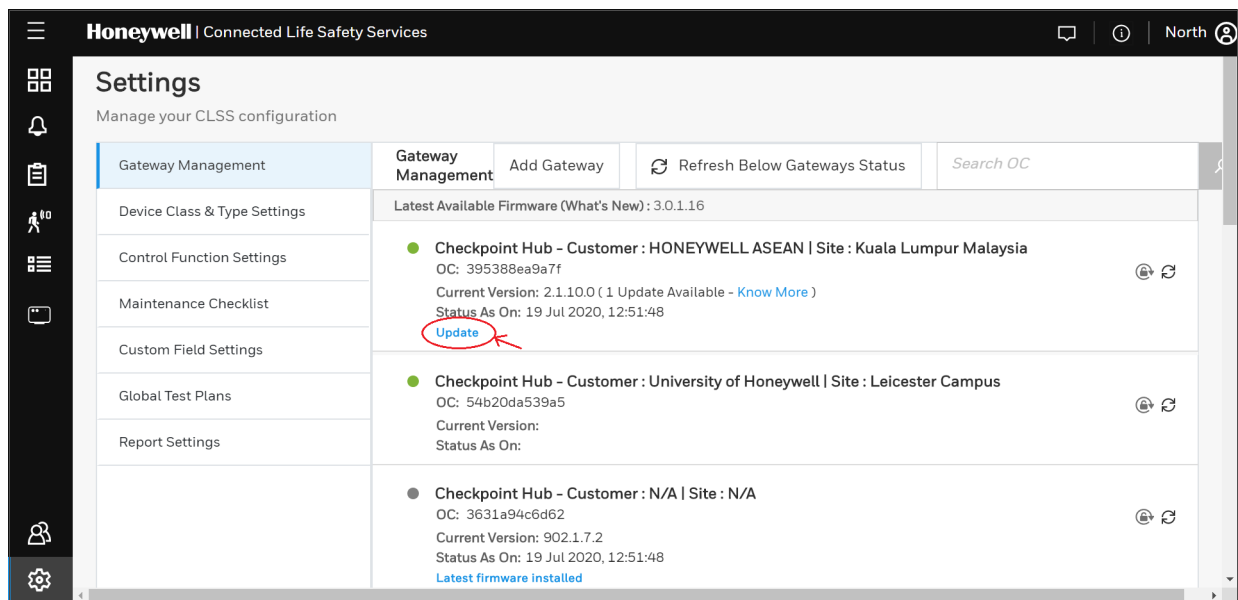


Figure 6.1: Firmware Upgrade

6.1.3 To Locally Upgrade with a PC

1. On the gateway side, connect an Ethernet cable to the Ethernet port (J3). The port is labeled as 2 in [Figure 4.3](#).
2. On the configuration computer side, connect the Ethernet cable to the configuration computer's Ethernet port.
3. On the gateway board, find the S6 button.
4. To switch to the configuration mode, press and hold the S6 button for a minimum of 6 seconds, and then release it. The LED indicator DL3 turns ON and SOLID, indicating that the configuration is enabled.
5. Open the Chrome browser and enter the following IP address for the configuration tool: **https://192.168.10.190:9443/config/index.html**
6. In the **Sign In** page, enter the password.



NOTE:The default password is: Welcome123

7. In the list of settings options, click **Diagnostic**.
8. In the **GATEWAY FIRMWARE UPGRADE** section, click **Choose File**.
9. Select the firmware image file and click **Choose**.
10. Once the chosen file is uploaded, click **Upgrade**.

6.1.4 To Verify the Upgrade

1. After the restart, log into the configuration tool.
2. Click **Diagnostic**.
3. Click **About** and verify that the new version of the gateway firmware is shown.

6.1.5 LED Indications During the Upgrade

While the gateway is downloading the firmware, the Green-color LED indicator DL4 will be ON.

If an LED is indicating differently, refer [Table 2.2](#) to determine the operational status. If necessary, refer to the [6.2, "Troubleshooting"](#) section to fix the problem or contact Honeywell Technical Support.

6.2 Troubleshooting

Issues that may occur during the gateway’s operation can be resolved on your own using the tables below or by contacting Honeywell Technical Support. The issues can be either LED-indicated issues or other issues.

6.2.1 To Troubleshoot LED-Indicated Issues

When an LED status indicates issues, refer to the below table to determine their possible fixes.

Table 6.1: LED-Indicated Issues and Possible Fixes

| SOM: Power LED-Indicated Issues | | |
|-----------------------------------|--|---|
| Power LED Status | Other LEDs’ Status | Possible Fixes |
| OFF | All other LEDs are OFF | <ul style="list-style-type: none"> Ensure that the gateway board’s power source is supplying the required 24V DC power. |
| ON | All other LEDs are OFF | <ul style="list-style-type: none"> Do the following: <ol style="list-style-type: none"> Remove all the connected cables. Wait for one minute. Reconnect all the cables. Ensure that the gateway board is getting its 24V DC power. If the above steps do not fix the issue, contact Honeywell Technical Support. |
| DL2: Trouble LED-Indicated Issues | | |
| Trouble LED Status | Other LEDs’ Status | Possible Fixes |
| ON and SOLID Amber | Any | <ul style="list-style-type: none"> It is a critical issue. Contact Honeywell Technical Support. |
| Flashing Amber once per second | <ul style="list-style-type: none"> DL3 The panel LED is OFF DL4 The <i>CLSS Site Manager</i> LED is flashing once per second | Check the following and correct if necessary: <ul style="list-style-type: none"> The cable connections at the gateway’s port and at the panel’s port The cable connecting the gateway board and the panel |
| Flashing Amber once per second | <ul style="list-style-type: none"> DL3 The panel LED is flashing once per second DL4 The <i>CLSS Site Manager</i> LED is OFF | Check the following and correct if necessary: <ul style="list-style-type: none"> Internet connectivity Eth1 cable connections at the gateway board side and at the panel side The Eth1 cable |
| DL3: Panel LED-Indicated Issues | | |
| Panel LED Status | Other LEDs’ Status | Possible Fixes |
| OFF | <ul style="list-style-type: none"> DL2 The Trouble LED is OFF | Check the following and correct if necessary: <ul style="list-style-type: none"> The cable connections at the gateway board side and at the panel side The Eth2 cable connecting the gateway board and the panel |

Table 6.1. LED-Indicated Issues and Possible Fixes (Continued)

| DL4: CLSS Site Manager LED-Indicated Issues | | |
|--|---|---|
| CLSS Site Manager LED Status | Other LEDs' Status | Possible Fixes |
| Flashing Green every 0.25 second | <ul style="list-style-type: none"> • DL3 The panel LED is flashing once per second • DL2 The Trouble LED is OFF | <ul style="list-style-type: none"> • Associate the gateway board with the user account. • Ensure that the user account is active. • Ensure that the panel's date and time are correct. |

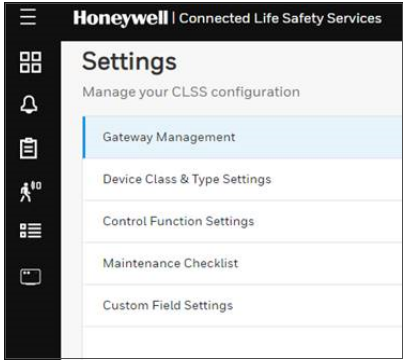

| DL5: Wireless LED-Indicated Issues | | |
|---|--|---|
| Wireless LED Status | Other LEDs' Status | Possible Fixes |
| OFF | <ul style="list-style-type: none"> • DL3 The panel LED is flashing once per second • DL4 The <i>CLSS Site Manager</i> LED is OFF | <ul style="list-style-type: none"> • Ensure that the WLAN settings in the gateway configuration tool are correct. • Ensure that the building's IP network has Internet and <i>CLSS Site Manager</i> connectivity. |

| DL6: Mobile LED-Indicated Issues | | |
|---|--|--|
| Mobile LED Status | Other LEDs' Status | Possible Fixes |
| OFF | <ul style="list-style-type: none"> • DL3 The panel LED is flashing once per second • DL4 The <i>CLSS Site Manager</i> LED is OFF | <ol style="list-style-type: none"> 1. On the gateway board, find the S8 button. To find the S8 button, refer to Figure 2.1. 2. Press the S8 button until the LED indicator DL6 flashes fast, indicating enabled mobile connectivity. |

6.2.2 To Troubleshoot Other Issues

If there are issues, which are not shown by the LEDs, refer to the below table to determine their possible fixes.

| Events-Related Issues | | |
|---|--|--|
| Issue Description | Possible Causes | Possible Fixes |
| Panel events are not displayed on the <i>Connected Life Safety Services App</i> | The gateway is dissociated. | Associate the gateway board with the user account. |
| | The user account is not associated with the gateway. | Ensure that the user account is active. |
| | The panel's date and time are incorrect. | Ensure that the panel's date and time are correct. |

| Events-Related Issues | | |
|--|--|--|
| Issue Description | Possible Causes | Possible Fixes |
| There is a need to reset the default password of the <i>Gateway Configuration Tool</i> | Forgot the <i>Gateway Configuration Tool's</i> password | <p>To reset to the default password:</p> <ol style="list-style-type: none"> 1. Log into the <i>CLSS Site Manager</i>: https://www.fire.honeywell.com 2. Click on the settings icon at the bottom-left section. 3. Click Gateway Management in the Settings section.  <ol style="list-style-type: none"> 4. Find the gateway whose configuration tool password needs to be reset. 5. To ensure that the gateway is online, check that there is a green icon before the gateway name. 6. Click on the reset password icon at the right-side of the gateway name.  <ol style="list-style-type: none"> 7. To confirm the reset, click CONTINUE on the message displayed. 8. Wait for the confirmation message. 9. Log in using the default password: Welcome123 |
| There is a need to reset the gateway board to its factory default settings | An unusual situation requires reverting to factory default settings. | Contact the Honeywell Tech Support for a guided procedure. |
| The CLSS App could not pair with the gateway. | The gateway firmware is not updated to 2.1.11.16 or above. | Upgrade the firmware to 2.1.11.16 or above. |
| Trouble IN SYSTEM ANN-PRI COMM FAULT DDEV #: ALL DEVICES | The ANN-PRI communication cable is not connected to the panel. | Connect the ANN-PRI communication cable with the panel. |

Section 7: Modbus Communications

The CLSS Gateway can use a third-party client to monitor the nodes inside a Modbus LAN network, and send alarm and event data of these nodes for the CLSS users.



NOTE: The Modbus interface provides supplementary data to the third party client.



NOTE: The Modbus details in this section are related to the NOTIFIER-UL panel.

7.1 Operation

The CLSS Gateway acts as a slave device to a Modbus master application and offer the Modbus monitoring functionalities to the CLSS Gateway users.



NOTE: The Modbus master application communicates with one or more panels over an NFN or a high-speed NFN network.

7.2 Functionality

With Modbus configurations the CLSS Gateway can:

- Communicate with an NFN network through an HS-NCM or NCM
- Directly connect to a single FACP in an NFN network
- Support Modbus Application Protocol Specification V1.1b.
- Monitor up to 10 FACPs.
Note: Additional FACPs require additional CLSS Gateways to the NFN network.
- Support a maximum of 2 Modbus clients or masters.

7.3 Recommended Cybersecurity Practices

- Follow the highly-recommended cybersecurity practices specified in the *Cybersecurity Manual* (LS10217-000NF-E).



CAUTION: FAILURE TO COMPLY WITH THE RECOMMENDED SECURITY PRACTICES IS A CYBERSECURITY RISK TO YOUR SYSTEM.

- Ensure that all the network security best practices discussed in [Section 3, “Security Recommendations”](#) are followed.

7.4 Required Software

- Chrome™
- Java™ version 6 or above

7.5 IP Requirements

7.5.1 IP Port Settings

The following IP ports must be available for the CLSS Gateway:

Table 7.1: Required IP Ports

| Port | Type | Direction | Purpose |
|------|------|-----------|-------------------------|
| 80 | TCP | In | Web Based Configuration |
| 443 | TCP | In | HTTPS Communications |
| 502 | TCP | In | Modbus |
| 4016 | TCP | In | Upgrades |

7.5.2 IP Restrictions

The following restrictions apply:

- The CLSS Gateway must have a static IP address. Dynamic Host Configuration Protocol (DHCP) is *not* supported.
- Web access via an HTTP proxy server is *not* supported.

7.6 Bandwidth Calculation

Use the following information to calculate the network bandwidth CLSS Gateway usage requires and how it will impact the network.

Table 7.2: Total Required Bandwidth

| For TCP Request | |
|---|-------|
| Description | Bytes |
| Ethernet Header | 14 |
| IP Header | 20 |
| TCP Header | 20 |
| MBAP Header | 7 |
| Message—5 bytes Function code (1) + Start Address (2) + Quantity of Registers (2) | 5 |
| Total Bytes | 66 |

| For TCP Response | |
|--|-------|
| Description | Bytes |
| Ethernet Header | 14 |
| IP Header | 20 |
| TCP Header | 20 |
| MBAP Header | 7 |
| Message—Function code (1) + Byte Count (1) + Max 100 registers of each 2 Bytes (200) | 202 |
| Total Bytes | 263 |

Requirements for the Calculation

- One request and response pair requires 329 Bytes (66 + 263).
- If a client is polling at one second intervals, then request and response are both possible in one second.
- A request and response pair creates network traffic of 329 Bytes per second (329 x 1).
- In other words, a request and response pair creates network traffic of 2632 bits per second (329 x 8).
- Therefore, the network must be able to accommodate at least 0.0027 Mbps data flow.
- Once every five seconds, an analog request adds a small amount of network traffic.
- Formula for CLSS Gateway network bandwidth requirement based on polling rate:

Bandwidth Requirement = $(329 \times (1000 / \text{polling rate in milliseconds}) \times 8) / (10^6)$ Mbps

7.7 System Architecture

An Internet or Intranet IP network connection is needed for the architectures described here.

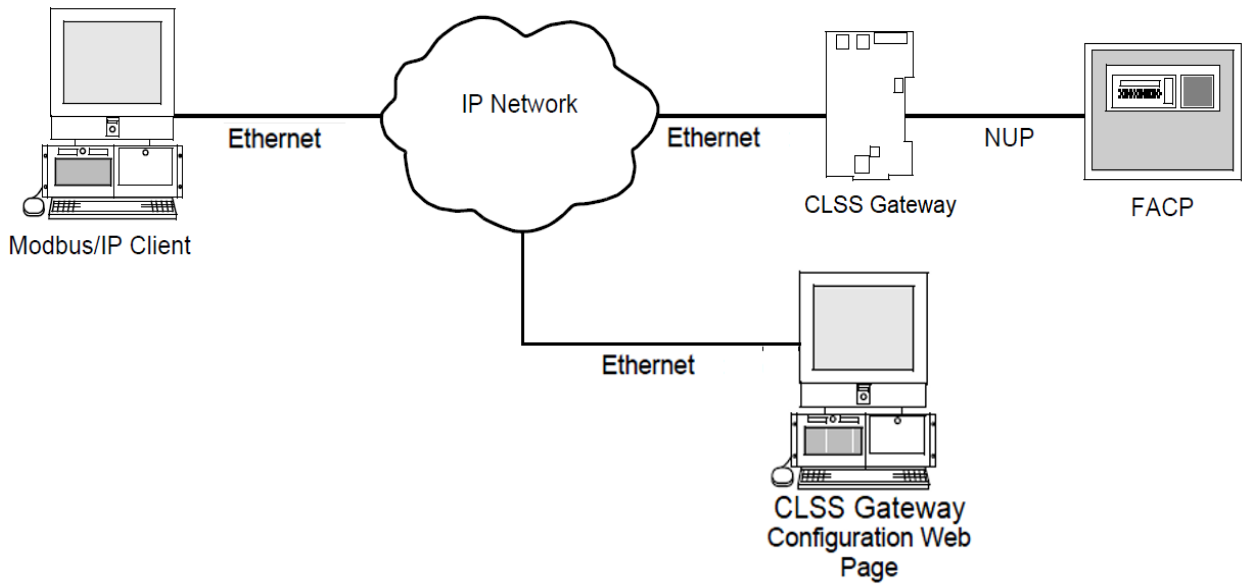


Figure 7.1: Single Panel Architecture

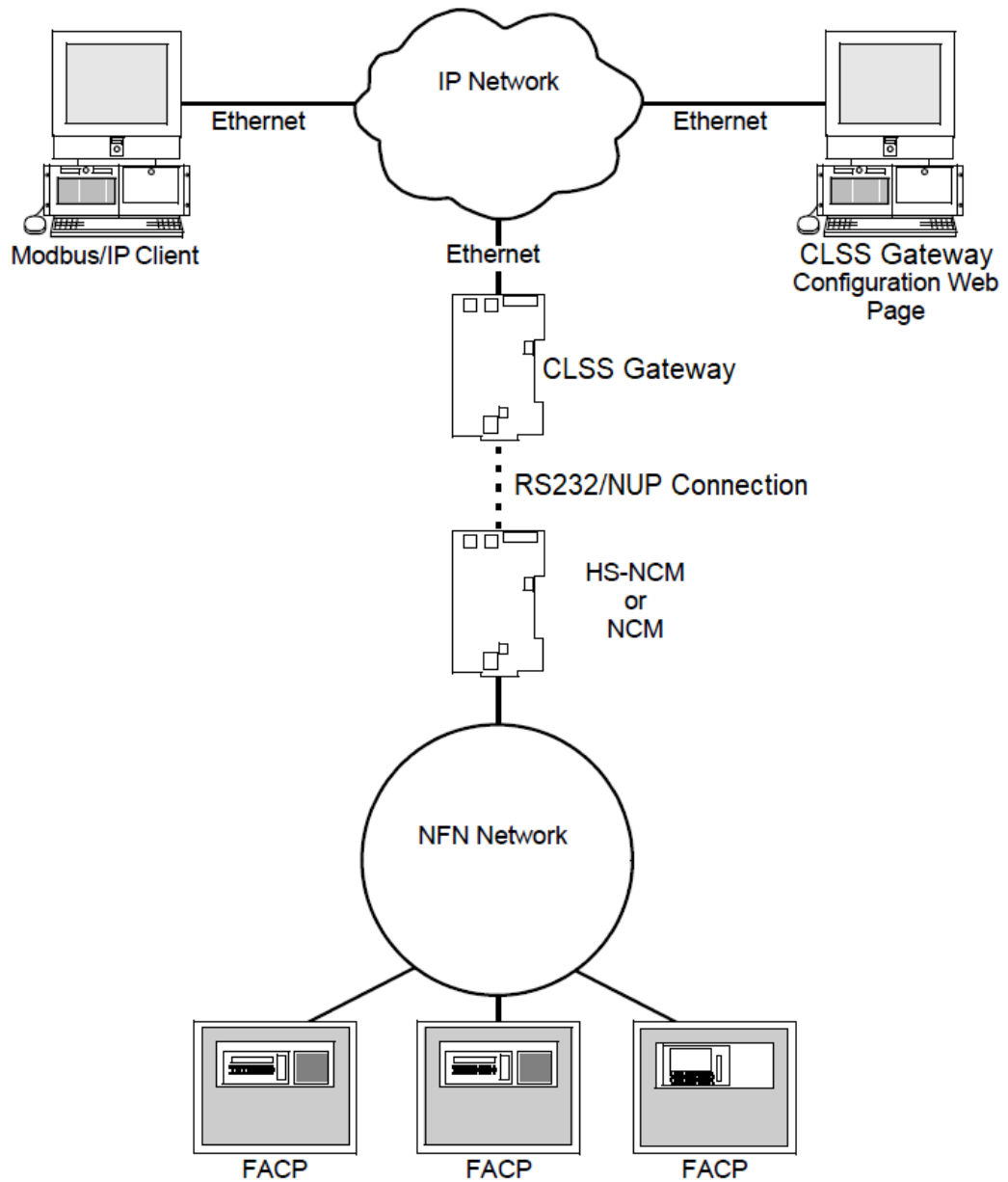


Figure 7.2: NFN Network Architecture

7.7.1 Redundancy

A redundant gateway is a second gateway, which communicates with a Modbus client.



CAUTION: THE FIRST AND SECOND GATEWAYS MUST HAVE DIFFERENT NODE NUMBERS AND DIFFERENT IP ADDRESSES.

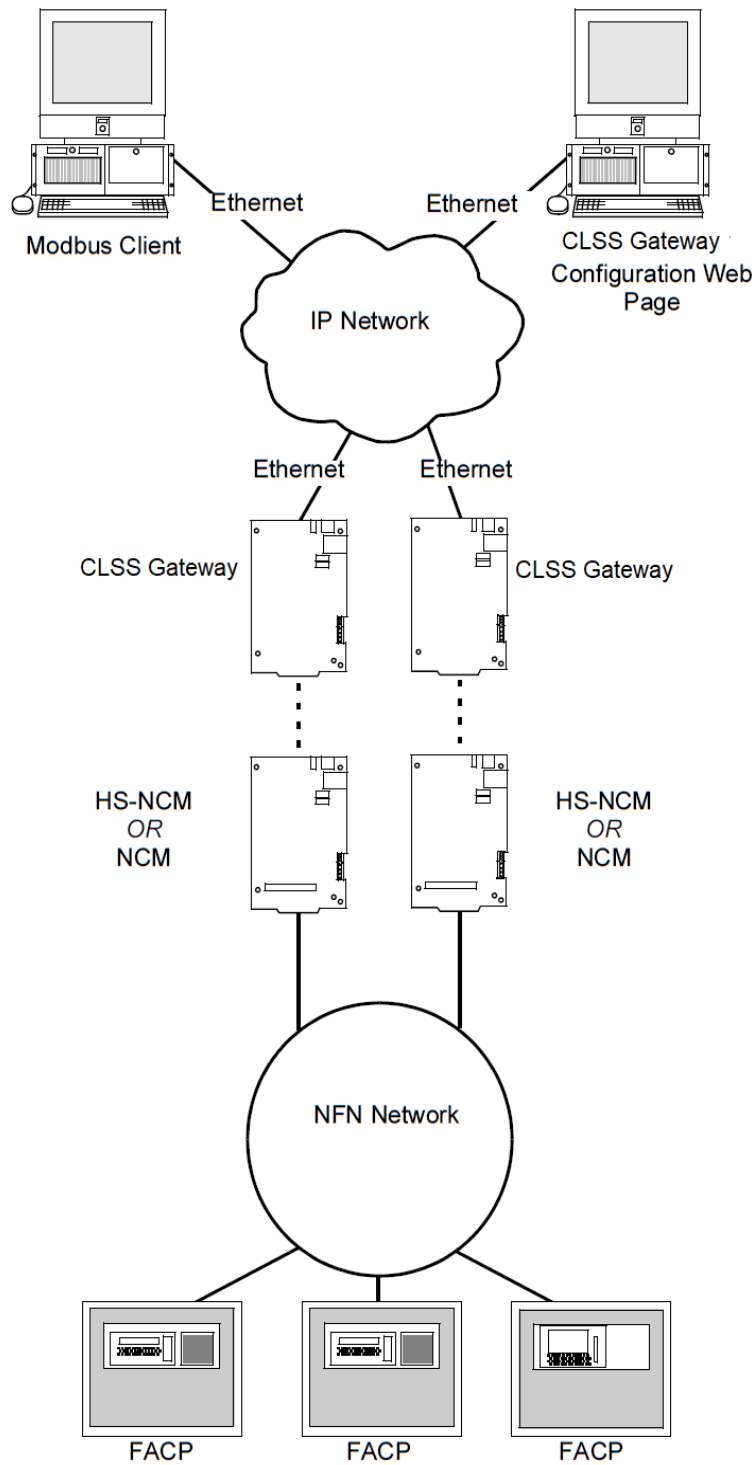


Figure 7.3: Redundant CLSS Gateways

7.8 Replacing the Modbus Gateway (Modbus-GW)

Following changes occur when the CLSS Gateway replaces the Modbus Gateway in the network.



NOTE: To know the Modbus Gateway values of the following, refer to the document: *LS10015-000NF-E Rev. C2*.

■ The Mapping of Registers

The CLSS Gateway and the Modbus Gateway have different mapping of registers.

Example:

The register range for loop-1 detectors:

In the Modbus Gateway: 40001 to 40200

In the CLSS Gateway: 40001 to 40300

Change the client-side scripting as required to change to the registry mapping of the CLSS Gateway.

For register mapping details for the CLSS Gateway, refer to the [7.22 "Register Mapping"](#) section.

■ Device Types

The device types are different for these two gateways.

Example:

Device Type value of Heat detector:

In the Modbus Gateway: 1

In the CLSS Gateway: 0100H

For device type details for the CLSS Gateway, refer to the [7.31 "Device Types"](#) section.

■ System Troubles

There are new troubles in the CLSS Gateway, and some of the system trouble names are different.

Example 1: New Troubles

In the CLSS Gateway: 460016-12th bit is *Workstation Failure*.

Example 2: Different trouble name

In the Modbus Gateway: The *General PS Fault* and the *Power Supply Trouble* are two different events.

In the CLSS Gateway: The 460015 - 8th bit is one single event for these two.

For system trouble details for the CLSS Gateway, refer to the [Table 7.33, "System Troubles Register Map"](#).

7.9 Using Both the CLSS Gateway and the Modbus Gateway

Ensure the following:

- The *Node Number* of the CLSS Gateway should be different from other gateways in the network.
- The *IP address* of the CLSS Gateway should be different from other gateways and devices in the network.



NOTE: The changes described in the [7.8 "Replacing the Modbus Gateway \(Modbus-GW\)"](#) section are applicable for this setup also.

7.10 Agency Listings and Approvals

- UL/ULC Listed: S35608
- CSFM: 7300-1637:0504
- FDNY: COA#000121, COA#000122

7.10.1 Agency Restrictions and Limitations

- CLSS Gateway is UL 864 and ULC-S527 listed for supplementary use only.

7.11 Standards

■ Compliance

This product has been investigated to, and found to be in compliance with, the following standards:

Underwriters Laboratories

- UL 864 - Control Units for Fire Alarm Systems, Tenth Edition

Underwriters Laboratories Canada

- CAN/ULC S527-19 - Standard for Control Units for Fire Alarm Systems, Fourth Edition

■ Installation

This product is intended to be installed in accordance with the following:

Local

- AHJ - Authority Having Jurisdiction

National Fire Protection Association

- NFPA 70 - National Electrical Code
- NFPA 72 - National Fire Alarm and Signaling Code

Underwriters Laboratories Canada

- CAN/ULC S527 - Installation of Fire Alarm Systems
- CAN/ULC S561 - Installation and Services for Fire Signal Receiving Centres and Systems

Canada

- CSA C22.1 - Canadian Electrical Code, Part I, Safety Standard for Electrical Installations

7.12 Compatible Equipment

The CLSS Gateway is compatible with the following equipment:

Table 7.3: CLSS-Compatible Equipment List

| Type | Equipment |
|----------------|---|
| Fire Panels | <ul style="list-style-type: none"> • NFS-320 • NFS-640 • NFS2-640 • NFS-3030 • NFS2-3030 • AFP2800 • AFP 3030 • XLS 120 • XLS 140-2 • XLS 2000 • XLS 3000 • N16 (INSPIRE) |
| Network Cards | <ul style="list-style-type: none"> • NCM-W, NCM-F • HS-NCM-W, HS-NCM-SF, HS-NCM-MF, HS-NCM-WSF, HS-NCM-WMF, HS-NCM-MFSF • NFN-GW-PC-NHW-2, HS-NCM-WMF-2, HS-NCM-WSF-2, HS-NCM-W-2 |
| Other Products | <p>Unmonitored but network compatible.</p> <ul style="list-style-type: none"> • DVC • NCA-2 • NCD • NWS-3 • BACNET-GW-3 • NFN-GW-PC-HNW-2 • NFN-GW-EM-3 • PC NFN Gateways: <ul style="list-style-type: none"> • NFN-GW-PC-F • NFN-GW-PC-W • NFN-GW-PC-HNMF • NFN-GW-PC-HNSF • NFN-GW-PC-HNW • VESDA-HLI-GW |

7.13 Modbus Feature Activation

Purchase the required number of Modbus support on *CLSS Site Manager* and then activate that feature in CLSS App.



NOTE: Purchase should be within the number of tokens available.

7.13.1 To Purchase the Modbus Support

1. Log onto *CLSS Site Manager*.
2. Click on your account name and select **Manage Access**.

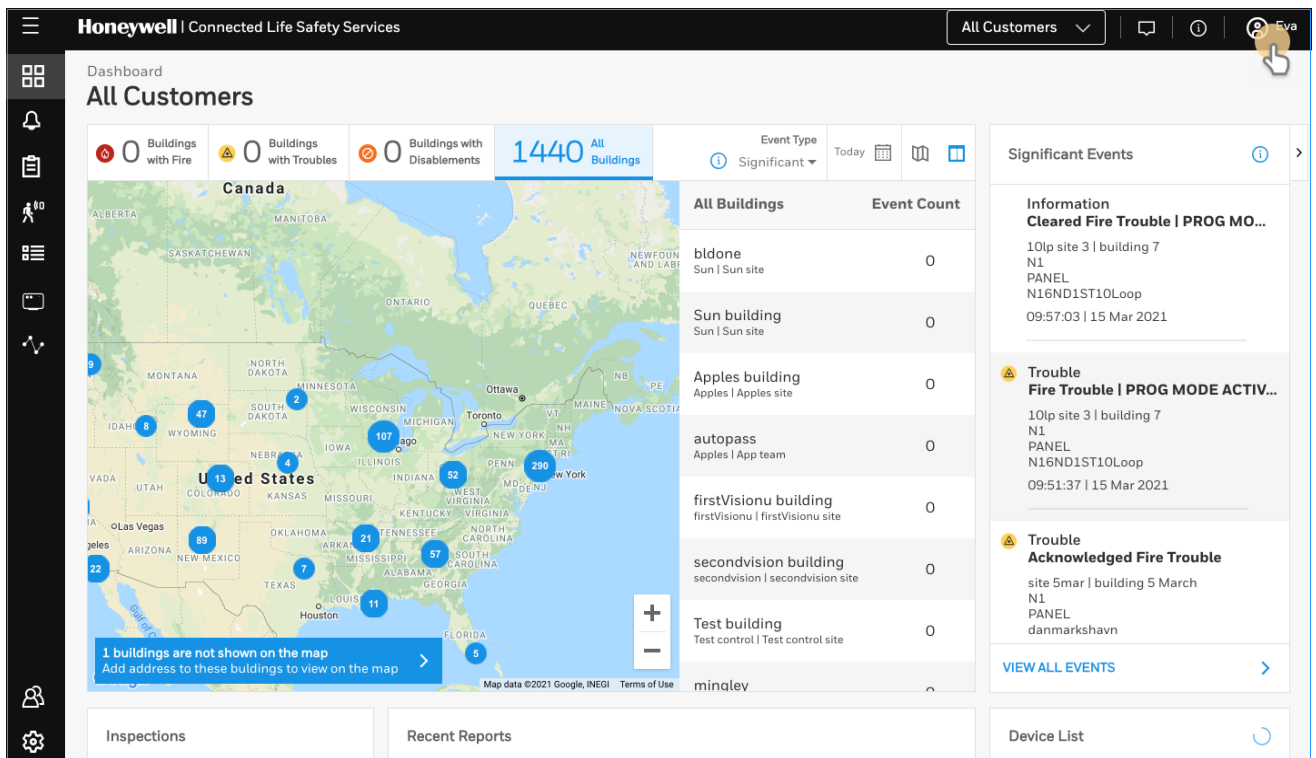


Figure 7.4: Selecting Manage Access

3. Click **Features** on the **Manage Access** page.
4. Click **Gateway** under the **Features** section.
5. Note down the purchased number under **Available Features**.
6. Click **PURCHASE** at the top right side.

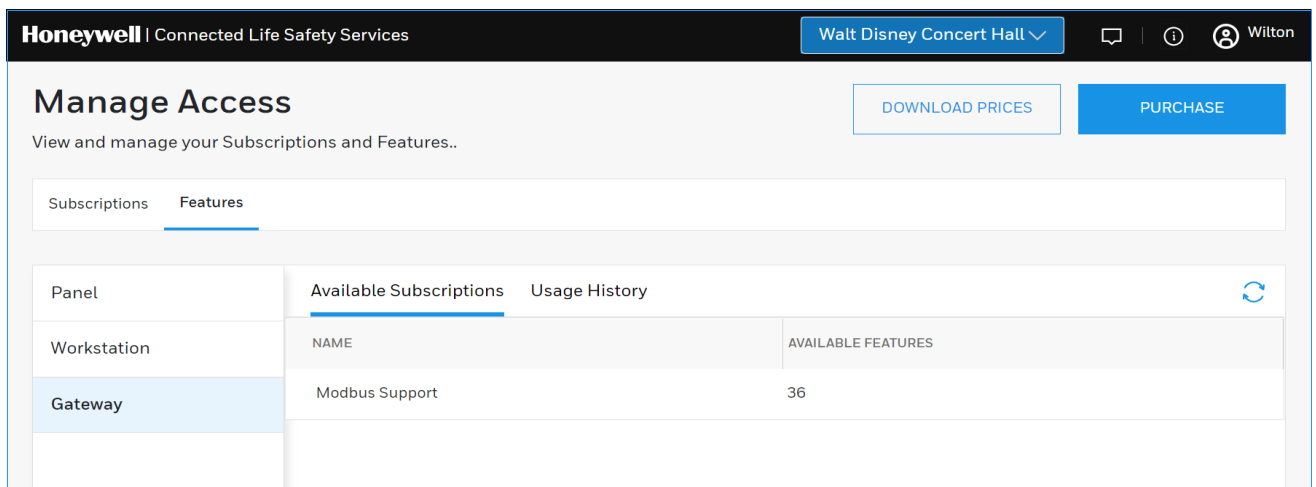


Figure 7.5: Purchasing the Modbus Support

7. Scroll down to find **Modbus Support** in the **Features** tab.
8. Enter the number of support required in the **Modbus Support** field.
9. Click **PURCHASE**.
10. Read the **Confirmation** message and if acceptable, click **CONFIRM**.
Or
Click **CANCEL** and repeat the steps from 8 to 10.
11. Wait for the purchase to complete and refresh the page, if required.
12. Verify that the purchased number under **Available Features** is correct.

7.13.2 To Activate the Modbus Support



NOTE:

- The gateway must be already installed. If not, install the fixed gateway.
- All the network settings should be configured while installing.

1. Tap **Perform Feature Activation** on the CLSS App's welcome message.

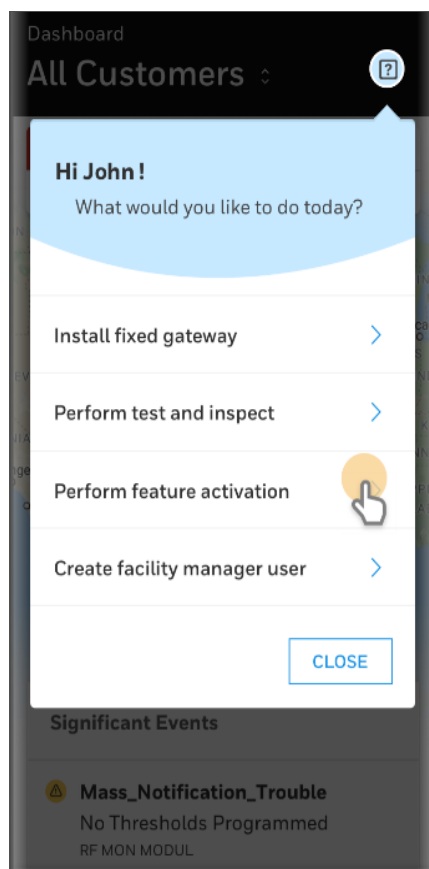


Figure 7.6: Feature Activation: The First Step

2. Tap **Fixed Gateways**.
3. Select the site of the gateway.
4. Find and tap the OC of the gateway.
5. Tap **ADD ACTIVATION**.
6. Tap **Modbus Support** under the **One Time Activations**.
7. Tap **ACTIVATE**.
8. Wait for the activation successful message.

7.14 Installation and Configurations

The CLSS Gateway can communicate with the Modbus client in an Ethernet LAN.

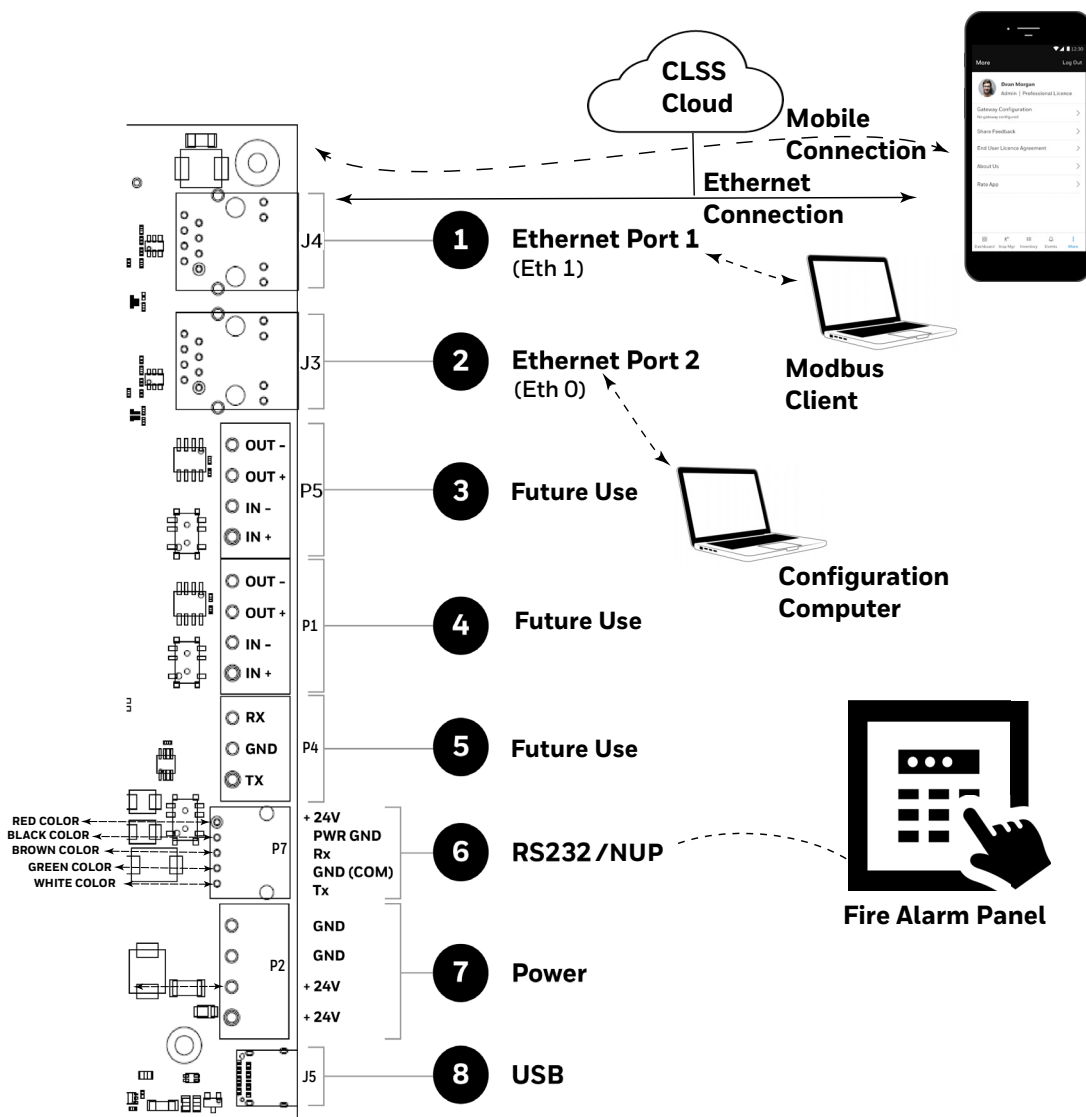
7.15 The IP Settings

The following information applies to IP settings:

- You can use only the *eth1* port for connections to Modbus clients. For more details, refer to [7.17 "To Configure the Modbus Settings"](#).
- Each CLSS Gateway is shipped with a default node number of 235.
- The computer used to configure the CLSS Gateway must establish an IP connection to the gateway. Consult with a network administrator if unsure how to make this connection.
- Connecting more than one CLSS Gateway prior to reconfiguring the IP address will result in an IP address conflict.

7.16 To Connect with the Modbus Client

1. At the CLSS Gateway side, connect an Ethernet cable to the Ethernet Port 1.



2. At the Modbus client side, connect the other end of the Ethernet cable to the system running the Modbus client.

7.17 To Configure the Modbus Settings

1. On the CLSS Gateway board, find the S6 button.
2. Press the S6 button for a minimum of 6 seconds and then release it. It will switch the gateway to configuration mode.
The LED indicator DL3 turns ON and SOLID indicating that the configuration is enabled.
3. Connect the Ethernet cable to *Eth0* for enabling web configuration.



NOTE: The web configuration is available only on *Eth0*.

4. Open the Configuration Computer connected to the *Eth0* port of the gateway.



NOTE: The static IP of the *Eth0* port is *192.168.10.190*.

5. In the Chrome browser, enter the following URL:
`https://192.168.10.190:9443/config/index.html`
6. Do the following if any security warning is shown. Otherwise, go to step 7.
 1. Click the *Advanced* link below the error message.
 2. Agree to proceed.
7. In the **Gateway Configuration Tool** page, enter the password.



NOTE: The default password is: *Welcome123*

8. Go to the **Network Settings** in the **Gateway Settings** section.
9. Assign the *Eth1* port with a static IP address for the Modbus connection.
10. Connect the Ethernet cable between the *Eth1* port of CLSS gateway and its LAN device.
11. Find and click **Modbus Settings** in the **Gateway Settings** section.

Honeywell | Gateway Configuration Tool
LOGOUT

Gateway Configuration

Configure gateway hardware settings

Gateway Settings

Panel List ▼

Network Settings

Modbus Settings

Alarm Transmission

POTS Configuration

Central Station Configuration

Diagnostic

Change Password

MODBUS GATEWAY SETTING

Enable Modbus Functionality Check to enable Modbus Functionality

Authorized Client IP

Gateway Unit ID

Analog Value Timeout

NODE MAPPING

Show all nodes ▼

12. In the **MODBUS GATEWAY SETTING** page, provide the required details for the Modbus client.

Table 7.4: Settings for Modbus Client Communications

| Field | Description |
|----------------------|--|
| Authorized Client IP | <p>This is an optional security feature.</p> <ul style="list-style-type: none"> Enter the authorized client IP address. The gateway only responds to requests from the client at that IP – no other Modbus clients may communicate with the gateway. However, any computer running a browser in the local network will still be able to access the CLSS Gateway configuration web page as normal. <p>Or</p> <ul style="list-style-type: none"> Enter 0.0.0.0 to allow up to 2 clients to connect at a given time. |
| Gateway Unit ID | <p>Displays the unit ID that the CLSS Gateway uses in the Modbus network. This is a configurable property of the nodes. By default, the Modbus Unit ID for a monitored node is set to be the same as the NFN Node ID.</p> <p>If for any reason the unit ID needs to be changed, click the value and enter the new unit ID number. Since each unit ID in the Modbus network needs to be unique, change this number only if there is a conflict in the unit IDs in the Modbus network.</p> <p>Note: Each of the 240 possible nodes on the NFN network (except for gateways, web servers, and DVCs) is automatically assigned a Modbus Unit ID. When a new unit ID number for a node is entered, the old unit ID number is reassigned to whichever node previously used the new unit ID number.</p> <p>However, the CLSS Gateway configuration web page does accept a new unit ID number that is currently being used by a monitored node. In order to reassign a unit ID number used by a monitored node, first assign a new unit ID number for the monitored node.</p> |
| Analog Value Timeout | <p>Enter the minimum frequency (in seconds) at which the CLSS Gateway expects to receive continuing polls from clients seeking analog values from 4–20 mA devices.</p> <p>When a client that had been polling a set of analog values fails to re-poll the values within the time out period, the CLSS Gateway stops polling the points in question. Once the time out period expires without the CLSS Gateway receiving a repeated poll, any further poll received will be treated as a new poll, and the first read will be considered an initialization read.</p> <p>Default value is 15 seconds.</p> |
| NODE MAPPING | |
| Show All Nodes | <ul style="list-style-type: none"> Select Yes to display all the nodes in the network. Select No to display only the nodes that the panel monitors in the network. |
| Node Status | Shows the operational status of each nodes displayed. It would be <i>Online</i> or <i>Offline</i> . |
| Node ID | Displays the number of each node in the NFN network. |
| Node Type | Shows the brand name of the node. For example, NFS2-3030. |

Table 7.4: Settings for Modbus Client Communications (Continued)

| Field | Description |
|-----------------------------|---|
| Node Unit ID | <p>Displays the unit ID that each node uses on the Modbus network.</p> <p>If for any reason the node unit ID needs to be changed, click the value and enter the new Modbus network unit ID number (1–240). Since each unit ID in the Modbus network needs to be unique, change this number only if there is a conflict between unit IDs in the Modbus network.</p> <p>If a unit ID number is changed to a number already assigned to another node, the node currently having that unit ID number swaps the unit ID number with the node that was changed.</p> <p>Example: The node assigned Unit ID #214 is changed to be Unit ID #5. The result is that the node that was Unit ID #214 is now #5 and the node that was Unit ID #5 is now #214.</p> <p>However, the CLSS Gateway configuration web page does accept a new unit ID number that is currently being used by a monitored node. In order to reassign a unit ID number used by a monitored node, first assign a new unit ID number for the monitored node.</p> <p>Notes:</p> <p>The <i>Unknown</i> nodes can only be seen in the <i>Show All Nodes</i> mode.</p> <p>If an <i>Unknown</i> node comes on line and is found to be of the wrong type for the CLSS Gateway to monitor, its Monitored field is automatically set to <i>No</i>.</p> <p>Some nodes in the node list are not usable by the CLSS Gateway and therefore are not configurable and do not have a unit ID.</p> |
| Monitoring | <ul style="list-style-type: none"> • Select Yes to monitor the node. • Select No if the node is not to be monitored. <p>At a given time, up to 10 nodes* can be monitored.</p> <p>* Excluding the CLSS Gateway.</p> |
| MODBUS TOOLS | |
| Control Functionality | <ol style="list-style-type: none"> 1. Go to Modbus Tools in Modbus Settings. 2. Enable or disable as needed in the control functionality. 3. Read the UL Void message shown, if enabled. 4. Click Save to save it. 5. Wait until the CLSS Gateway shows the changes. |
| CSV REPORTS DOWNLOAD | |
| Actual Points | Click Download to download details of points (detectors and modules), which the panel monitors. The downloaded details will be in the CSV format. |
| All Points | Click Download to download details of monitored and unmonitored points. The downloaded details will be in the CSV format. |
| CONNECTED CLIENTS | |
| Show Connected Clients | Click Show to view all the clients connected to the Modbus master application. |

13. Click **SAVE**.

14. Press the S6 button again until the LED indicator DL3 changes from ON to flashing.



NOTE: The configuration changes are enabled only after the gateway changes from the configuration mode to operational mode.

7.18 To Configure the Modbus Client

1. Open the Modbus master application you are using.
2. Specify the IP address of *Eth1* port of the CLSS Gateway.
3. Specify the port that the Modbus client is using in the **Service Port** field.

7.19 Modbus Command Support

The CLSS Gateway supports the following Modbus commands:

- Read Input Registers (0x04)
- Read Holding Registers (0x03)
- Write Single register (0x06)
- Read Device Identification supported 43 / 14 (0x2B / 0x0E)

Exception Responses

The CLSS Gateway sends exception responses to its Modbus clients as appropriate (e.g., invalid command, invalid data, etc.). For more information, refer to [7.29 "Exception Responses"](#).

Modbus Addressing

The CLSS Gateway uses Modbus addressing within the following guidelines:

- The CLSS Gateway operates similarly to a Modbus bridge. Each CLSS Gateway can support up to ten panels on an NFN network. Each fire panel being addressed by the Modbus master on the NFN network is identified by the Unit ID.
- The Unit ID used in the CLSS Gateway must be in the range 1 to 240. This is a Modbus range limitation.
- The Unit ID should match the node number of the NFN node that is being addressed. For example, a Unit ID of 127 addresses NFN node 127.
- The CLSS Gateway communicates on standard Modbus IP port 502.



NOTE: Communication on Modbus IP port 502 is not configurable and is a Modbus norm.

- Standard register types and reference ranges are:
 - 0x Coil 000001–065536
 - 1x Discrete Input 10001–165536
 - 3x Input Register 300001–365536
 - 4x Holding Register 400001–465536

For more information on Modbus addressing, [See "Register Mapping" on page 61.](#)

7.20 CLSS Gateway Control Features

7.20.1 Supported Commands

Enabling control of the CLSS Gateway allows the user to modify the following commands:

- Acknowledge (Block or Alarm)
- Silence (Node)
- Reset (Node)
- Activate/Deactivate (Device or Zone)
- Enable/Disable (Device or Zone)

7.20.2 Enabling Control

CAUTION: UL LISTING
ENABLING CONTROL VOIDS THE UL LISTING OF THE CLSS GATEWAY.

CLSS gateway control is enabled through a web page-based configuration tool running on the gateway. Enable control as follows:

1. Start the web browser on a computer that is in the same IP network as the CLSS Gateway.
Note: Chrome is the recommended browser.
2. Enter the following URL in the browser:
<https://192.168.10.190:9443/config/index.html>
3. Do the following if any security warning is shown. Otherwise, go to step 4.
 - Click the **Advanced** link below the error message.
 - Agree to proceed.
4. In the **Gateway Configuration Tool** page, enter the password.
5. Go to **Modbus Tools** in **Modbus Settings**.
6. Enable or disable as needed in the control functionality.
7. Read the **UL Void** message shown, if it is enabled.
8. Click **Save**.
9. Wait until the CLSS Gateway shows the changes.
10. Check that the changes are correct.

7.20.3 Sending Commands

Send commands through the CLSS gateway by writing command values to the appropriate holding registers. For detailed register mapping information refer to the [7.22 "Register Mapping"](#) section. The following tables display the values representing all the command types for nodes, points, and zones.

Table 7.5: Node Commands

| Command | Value | Holding Register |
|---------|--------|------------------|
| Reset | 0x0001 | 20001 |
| Silence | 0x0002 | |

Table 7.6: Point Commands

| Command | Value | Holding Register |
|-------------|--------|--|
| Acknowledge | 0x0100 | Use Device/Module Holding Register Address |
| Disable | 0x0200 | |
| Enable | 0x0400 | |
| Activate | 0x0800 | |
| Deactivate | 0x1000 | |

Table 7.7: Zone Commands

| Command | Value | Holding Register |
|--------------|--------|-----------------------------------|
| Disable | 0x0200 | Use Zone Holding Register Address |
| Enable | 0x0400 | |
| Activate * | 0x0800 | |
| Deactivate * | 0x1000 | |

Table 7.7: Zone Commands

| Command | Value | Holding Register |
|---------|-------|------------------|
|---------|-------|------------------|

* Activate and Deactivate work only for output-controlled modules like control and relay.

Different panels support different zone types. Refer to [Table 7.8, "Zone Command Availability by Panel"](#) for information about zone types supported.

Table 7.8: Zone Command Availability by Panel

| Panel Type | General Zones | | Logic Zones | | Trouble/Release Zones | |
|------------|----------------|---------------------|----------------|---------------------|-----------------------|---------------------|
| | Enable/Disable | Activate/Deactivate | Enable/Disable | Activate/Deactivate | Enable/Disable | Activate/Deactivate |
| AFP-2800 | Yes | No | No | No | No | No |
| AFP-3030 | Yes | No | No | No | No | No |
| N16 | Yes | Yes | Yes | No | No | No |
| NFS-320 | Yes | No | No | No | No | No |
| NFS-640 | Yes | No | No | No | No | No |
| NFS2-640 | Yes | No | No | No | No | No |
| NFS-3030 | Yes | No | No | No | No | No |
| NFS2-3030 | Yes | Yes | Yes | No | No | No |
| XLS 120 | Yes | No | No | No | No | No |
| XLS 140-2 | Yes | No | No | No | No | No |
| XLS 2000 | Yes | No | No | No | No | No |
| XLS 3000 | Yes | Yes | Yes | No | No | No |

7.21 Analog Values and Trending

Trending of analog values is supported on all of the panels/networks 4–20 mA modules. The only limitation is that the gateway will only actively read analog values for up to 10 analog modules at a time. All the analog values on all the modules can be read as long as a separate poll is sent for these points in groups of up to 10 points at a time, following the rules outlined below. Refer to ["Analog Value Use Cases"](#) for clarity on this issue.

- Accept a poll for up to any 10 analog (4–20 mA) points per gateway.
- Requests for more points than this are rejected with an exception code.
- If any of the points in the request are not 4–20 mA modules then the gateway rejects the request with an exception code.
- The first poll for analog values is an initialization poll. This initialization poll informs the gateway to start acquiring analog values for these points at 5 second intervals.
- Points are only polled on the NFN if the 4–20 mA module is in at least the first level of alarm status. If the point is normal then the gateway returns a value of zero.



NOTE: The first response to an analog point poll is zero. This response is an initialization confirmation from the gateway.

- Upon receiving the initialization confirmation, the client can begin polling the analog points. The client should wait 5 seconds after the initialization request to insure that the CLSS Gateway has had enough time to get the analog values and load the registers. Thereafter the CLSS Gateway continues to poll the points. The analog value in the CLSS Gateway are updated no faster than once every 5 seconds.
 - Points are polled if the device is in at least the first level of alarm status. Zero is returned for devices not in alarm status.
 - When a point being polled enters normal status, polling for that point on the NFN is terminated and the analog value register for that point is filled with zeros.
- The CLSS Gateway ceases polling the analog points when:
 - The client does not make a request for these exact same points over a period defined in the Modbus Configuration Tool as “Analog Value Time Out”. The default is 15 seconds.
 - The gateway makes a request for a point (or points) that is not *exactly the same as the initial request*. The CLSS Gateway first sends an initial confirmation for the new set of analog points, and then begins polling those points at 5 second intervals.
- When a 4–20 mA module is in fault, the analog value register for that point is filled with zeros.

Analog Value Use Cases

Use Case 1: A client requests analog values from the points L1M1 through L1M10 every 10 seconds.

Result: The CLSS Gateway sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The CLSS Gateway sends back actual values on the second request from the client 5 seconds later. The CLSS Gateway continues to poll these devices as long as the client continues to send analog value requests for points L1M1 through L1M10 at a rate faster than the Analog Value Time Out.

Use Case 2: A client requests analog values from the points L1M1 through L1M10. After 10 minutes of polling on a 10 second interval, the client stops requesting analog values for these points.

Result: The CLSS Gateway sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The CLSS Gateway sends back actual values on the second request from the client 10 seconds later. The CLSS Gateway continues to poll these devices as long as the client continues to send analog value requests for points L1M1 through L1M10. When the client stops polling at 10 minutes, the CLSS Gateway will stop polling the NFN after the Analog Value Time Out expires.

Use Case 3: A client requests analog values from the points L1M1 through L1M10. After 10 minutes of polling on a 10 second interval, the client requests analog values from the points L1M20 to L1M22.

Result: The CLSS Gateway sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The CLSS Gateway sends back actual values on the second request from the client 10 seconds later. The Gateway continues to poll these devices as long as the client continues to send analog value requests for the points L1M1 through L1M10. When the client sends a request for analog values from the points L1M20 through L1M22, gateway waits till the timeout happens and then the CLSS Gateway immediately sends back zeros in response to the first analog value request from these points and starts polling L1M20 through L1M22. The CLSS Gateway only polls the points specifically requested.

Use Case 4: A client requests analog values from the points L1M1 through L1M10. After 10 minutes of polling on a 10 second interval, the client requests analog values from the points L1M5 through L1M12.

Result: The CLSS Gateway sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The CLSS Gateway sends back actual values in response to the second request from the client 10 seconds later. The CLSS Gateway continues to poll these devices as long as the client continues to send analog value requests for the points L1M1 through L1M10. When the client sends a request for analog values from the points L1M5 through L1M12, the gateway immediately sends back zeros in response to the first analog value request from points L1M11 and L1M12 (since these are newly requested points) and it sends back actual values in response to the continuing analog value requests for points L1M5 through L1M10 (since it already has been polling these points). The gateway stops polling points L1M1 through L1M4 and starts polling points L1M5 through L1M12.

Use Case 5: A client requests analog values from the points L1M1 through L1M15.

Result: The CLSS Gateway sends back an exception response because it can only process requests for up to 10 analog values at a time. The client should request and receive values for L1M1 through L1M10 and then send a request for L1M11 through L1M15. Note that the first request for analog values from a valid range of points is considered an initialization request, which returns zeros.

7.22 Register Mapping

7.22.1 Register Mapping Overview

The CLSS Gateway uses 16-bit registers. One Modbus Input register and one Modbus Holding Register are allocated for each device address. These registers represent a contiguous address mapping of all devices and points.



NOTE: You can reserve 300 registers for device type registers.

7.22.2 Point Status Holding Registers

Each of the point status holding registers are divided into an upper and lower byte as described below and in [Table 7.9, “Point Status Holding Register Bit Definitions”](#).

- **Upper Byte:** The upper byte contains general status information about the point.
- **Lower Byte:** The lower byte is primarily used when bit 11 in the upper byte is a ‘1’ (or active). When bit 11 is a ‘1’, [See “CLSS Gateway Active Event Code” on page 74](#). for detailed information about the active point. The lower byte will be all 0’s if the device is not in an active state.

Specifically, the lower byte contains the actual active event for this point. An active state is defined in this gateway as any Fire, Security, Critical Process, Medical, Mass Notification, or Supervisory alarm state.

If the point is not present in the panel programming, all bits in the lower byte will contain a ‘1’ or the value FFH, but the upper byte will contain a ‘0’.

The only possible active event type for zones is Non-Fire Activation (71H). See [“CLSS Gateway Active Event Code” on page 74](#).

Table 7.9: Point Status Holding Register Bit Definitions

| Bit No. | Upper Byte | | | | | | | | Lower Byte | | | | | | | |
|----------|---|----------|---------|----------|--------|--------|---------|----------------|--|---|---|---|---|---|---|---|
| | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Bit Name | Ack Block | Prealarm | Trouble | InActive | Active | Enable | Disable | Ack Fire Alarm | | | | | | | | |
| | When individual upper byte bits are set to 1, the following definitions apply: Ack Block (Bit 15): All events on this point, other than fire alarm, are acknowledged. Not applicable for zones. Prealarm (Bit 14): The point is in a prealarm state. Not applicable for zones. Trouble (Bit 13): The point is in a trouble state. Not applicable for zones. InActive (Bit 12): The point is not active. Active (Bit 11): The point is active and there will be an active event type in the lower byte. Enable (Bit 10): The point is enabled. Disable (Bit 9): The point is disabled. Ack Fire Alarm (Bit 8): The fire alarm on this point is acknowledged. Not applicable for zones. | | | | | | | | Active Event Code (When Bit 11 is set to 1, see 7.30 “CLSS Gateway Active Event Code” .) | | | | | | | |

The holding register addresses and the points contained in these addresses are detailed in [Table 7.10, “Point Status Holding Register Device/Module Addresses”](#). Each range of holding registers is used for either detectors or modules.

Table 7.10: Point Status Holding Register Device/Module Addresses

| Start Address | End Address | Address |
|---------------|-------------|-------------|
| 400001 | 400300 | L1D1–L1D300 |
| 400301 | 400600 | L1M1–L1M300 |
| 400601 | 400900 | L2D1–L2D300 |
| 400901 | 401200 | L2M1–L2M300 |
| 401201 | 401500 | L3D1–L3D300 |
| 401501 | 401800 | L3M1–L3M300 |
| 401801 | 402100 | L4D1–L4D300 |
| 402101 | 402400 | L4M1–L4M300 |
| 402401 | 402700 | L5D1–L5D300 |
| 402701 | 403000 | L5M1–L5M300 |
| 403001 | 403300 | L6D1–L6D300 |
| 403301 | 403600 | L6M1–L6M300 |
| 403601 | 403900 | L7D1–L7D300 |
| 403901 | 404200 | L7M1–L7M300 |
| 404201 | 404500 | L8D1–L8D300 |
| 404501 | 404800 | L8M1–L8M300 |
| 404801 | 405100 | L9D1–L9D300 |
| 405101 | 405400 | L9M1–L9M300 |

Table 7.10: Point Status Holding Register Device/Module Addresses (Continued)

| | | |
|--------|--------|---------------|
| 405401 | 405700 | L10D1–L10D300 |
| 405701 | 406000 | L10M1–L10M300 |

 **NOTE:** On the AFP-2800, output activation status is not reported to the CLSS Gateway and therefore the bits and event type will always indicate a non-active state.

7.22.3 Point Device Type Input Registers

 **NOTE:** If the point is not present in the panel programming, all bits in the byte will contain a value of 1 or *FFFFH*.

There are 6000 point device type holding registers. Each register address consists of two bytes representing a detector or module.

Table 7.11: Point Device Type Input Register Bit Definitions

| Bit No. | Upper Byte | | | | | | | | Lower Byte | | | | | | | |
|--|------------|----|----|----|----|----|---|---|------------|---|---|---|---|---|---|---|
| | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Device Types (see 7.31 "Device Types") | | | | | | | | | | | | | | | | |

Table 7.12: Input Register Addresses of the Point Device Types

| Start Address | End Address | Address |
|---------------|-------------|---------------|
| 300001 | 300300 | L1D1–L1D300 |
| 300301 | 300600 | L1M1–L1M300 |
| 300601 | 300900 | L2D1–L2D300 |
| 300901 | 301200 | L2M1–L2M300 |
| 301201 | 301500 | L3D1–L3D300 |
| 301501 | 301800 | L3M1–L3M300 |
| 301801 | 302100 | L4D1–L4D300 |
| 302101 | 302400 | L4M1–L4M300 |
| 302401 | 302700 | L5D1–L5D300 |
| 302701 | 303000 | L5M1–L5M300 |
| 303001 | 303300 | L6D1–L6D300 |
| 303301 | 303600 | L6M1–L6M300 |
| 303601 | 303900 | L7D1–L7D300 |
| 303901 | 304200 | L7M1–L7M300 |
| 304201 | 304500 | L8D1–L8D300 |
| 304501 | 304800 | L8M1–L8M300 |
| 304801 | 305100 | L9D1–L9D300 |
| 305101 | 305400 | L9M1–L9M300 |
| 305401 | 305700 | L10D1–L10D300 |
| 305701 | 306000 | L10M1–L10M300 |

7.22.4 Zones/Panel Circuits Status Holding Registers

Each of the zones/panel circuits status holding registers are divided into an upper and lower byte as described below.

- **Upper Byte:** The upper byte contains general status information about the zone or panel circuit.
- **Lower Byte:** The lower byte is primarily used when bit 11 in the upper byte is a '1' (or active). When bit 11 is a '1', See "[CLSS Gateway Active Event Code](#)" on page 74. for detailed information about the active zone or panel circuit. The lower byte will be all 0's if the zone/panel circuit is not in an active state.

Specifically, the lower byte contains the actual active event for this zone or panel circuit. An active state is defined in this gateway as any Fire, Security, Critical Process, Medical, Mass Notification, or Supervisory alarm state.

If the zone or panel circuit is not present in the panel programming, all bits in the lower byte will contain a '1' or the value 'FFH', but the upper byte will contain a '0'.

Table 7.13: Zones/Panel Circuits Holding Register Bit Definitions

| Bit No. | Upper Byte | | | | | | | | Lower Byte | | | | | | | |
|----------|---|----------|---------|----------|--------|--------|---------|----------------|--|---|---|---|---|---|---|---|
| | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Bit Name | Ack Block | Prealarm | Trouble | InActive | Active | Enable | Disable | Ack Fire Alarm | | | | | | | | |
| | When individual upper byte bits are set to 1, the following definitions apply: Ack Block (Bit 15): All events on this zone/panel circuit, other than fire alarm, are acknowledged. Prealarm (Bit 14): The zone/panel circuit is in a prealarm state. Trouble (Bit 13): The zone/panel circuit is in a trouble state. InActive (Bit 12): The zone/panel circuit is not active. Active (Bit 11): The zone/panel circuit is active and there will be an active event type in the lower byte. Enable (Bit 10): The zone/panel circuit is enabled. Disable (Bit 9): The zone/panel circuit is disabled. Ack Fire Alarm (Bit 8): The fire alarm on this zone/panel circuit is acknowledged. | | | | | | | | Active Event Type (When Bit 11 is set to 1, see 7.30 " CLSS Gateway Active Event Code ".) | | | | | | | |

The holding register addresses and the zones contained in these addresses are detailed in this table.

Table 7.14: Zones

| Zone Type | Register Address | Zone Address |
|-----------------|------------------|---------------------------|
| General Zones | 408001–410000 | Z 1,2,3,4,5,6,7,8,...2000 |
| Logic Zones | 410001–412000 | Z 1,2,3,4,5,6,7,8,...2000 |
| Trouble Zones | 412001–412100 | Z 1,2,3,4,5,6,7,8,...100 |
| Releasing Zones | 412101–412200 | Z 1,2,3,4,5,6,7,8,...100 |

The holding register addresses and the panel circuits contained in these addresses are detailed in [Table 7.15, "Panel Circuits"](#).

Table 7.15: Panel Circuits

| Register Address | Panel Circuits |
|------------------|----------------|
| 414001–414008 | P1.1–P1.8 |
| 414009–414016 | P2.1–P2.8 |
| 414017–414024 | P3.1–P3.8 |
| 414025–414032 | P4.1–P4.8 |
| 414033–414040 | P5.1–P5.8 |

Table 7.15: Panel Circuits (Continued)

| | |
|---------------|--------------|
| 414041–414048 | P6.1–P6.8 |
| 414049–414056 | P7.1–P7.8 |
| 414057–414064 | P8.1–P8.8 |
| 414065–414072 | P9.1–P9.8 |
| 414073–414080 | P10.1–P10.8 |
| 414081–414088 | P11.1–P11.8 |
| 414089–414096 | P12.1– P12.8 |

The maximum panel circuit points by fire panel is described in [Table 7.16, “Supported Circuits by Panel”](#).

Table 7.16: Supported Circuits by Panel

| Panel | Max. Panel Circuits Points |
|-----------|----------------------------|
| NFS-320 | Not Supported |
| NFS-640 | 8 |
| NFS2-640 | Not Supported |
| NFS-3030 | 12 |
| NFS2-3030 | Not Supported |

7.22.5 Bell Circuits Status Holding Registers

■ NFS2-640 and NFS-320 Only

Each of the bell circuits status holding registers are divided into an upper and lower byte as described below and in [Table 7.9, “Point Status Holding Register Bit Definitions”](#).

- **Upper Byte:** The upper byte contains general status information about the bell circuit.
- **Lower Byte:** The lower byte is primarily used when bit 11 in the upper byte is a ‘1’ (or active). When bit 11 is a ‘1’, [See “CLSS Gateway Active Event Code” on page 74.](#) for detailed information about the active bell circuit. The lower byte will be all 0’s if the bell circuit is not in an active state.

Specifically, the lower byte contains the actual active event for this bell circuit. An active state is defined in this gateway as any Fire, Security, Critical Process, Medical, Mass Notification, or Supervisory alarm state.

If the bell circuit is not present in the panel programming, all bits in the lower byte will contain a ‘1’ or the value ‘FFH’, but the upper byte will contain a ‘0’.

Table 7.17: Zones/Panel Circuits Holding Register Bit Definitions

| Bit No. | Upper Byte | | | | | | | | Lower Byte | | | | | | | |
|----------|---|----------|---------|----------|--------|--------|---------|----------------|--|---|---|---|---|---|---|---|
| | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Bit Name | Ack Block | Prealarm | Trouble | InActive | Active | Enable | Disable | Ack Fire Alarm | | | | | | | | |
| | When individual upper byte bits are set to 1, the following definitions apply: Ack Block (Bit 15): All events on this bell circuit, other than fire alarm, are acknowledged. Prealarm (Bit 14): The bell circuit is in a prealarm state. Trouble (Bit 13): The bell circuit is in a trouble state. InActive (Bit 12): The bell circuit is not active. Active (Bit 11): The bell circuit is active and there will be an active event type in the lower byte. Enable (Bit 10): The bell circuit is enabled. Disable (Bit 9): The bell circuit is disabled. Ack Fire Alarm (Bit 8): The fire alarm on this bell circuit is acknowledged. | | | | | | | | Active Event Type (When Bit 11 is set to 1, see 7.30 "CLSS Gateway Active Event Code" .) | | | | | | | |

The holding register address and the bell circuit contained in the address is detailed in [Table 7.18, "Bell Circuit Holding Register Addresses"](#).

Table 7.18: Bell Circuit Holding Register Addresses

| Start Address | End Address | Device Address |
|---------------|-------------|----------------|
| 406001 | 406001 | Bell Circuit 1 |
| 406002 | 406002 | Bell Circuit 2 |
| 406003 | 406003 | Bell Circuit 3 |
| 406004 | 406004 | Bell Circuit 4 |

7.22.6 Bell Circuits Device Type Input Registers



NOTE: If the point is not present in the panel programming, all bits in the byte will contain a value of 1 or FFFFH.

Each bell circuits device type holding register address consists of two bytes as defined in [Table 7.19, "Bell Circuits Device Type Input Register Bit Definitions"](#) representing a bell circuit as shown in [Table 7.20, "Bell Circuit Device Type -Input Register Addresses"](#).

Table 7.19: Bell Circuits Device Type Input Register Bit Definitions

| Bit No. | Upper Byte | | | | | | | | Lower Byte | | | | | | | |
|---|------------|----|----|----|----|----|---|---|------------|---|---|---|---|---|---|---|
| | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Device Types (see 7.31 "Device Types") | | | | | | | | | | | | | | | | |

Table 7.20: Bell Circuit Device Type -Input Register Addresses

| Start Address | End Address | Device Address |
|---------------|-------------|----------------|
| 306001 | 306001 | BellCircuit1 |
| 306002 | 306002 | BellCircuit2 |
| 306003 | 306003 | BellCircuit3 |
| 306004 | 306004 | BellCircuit4 |

7.22.7 Panel Status Holding Register

The panel status holding register is divided into an upper and lower byte as described below and in [Table 7.21, “Panel Status Holding Register Bit Definitions”](#) representing one register address as shown in [Table 7.22, “Panel Status Holding Register Addresses”](#).

- **Silence:** The fire alarm control panel is silenced when this bit is set to 1.
- **Reset:** Not used.

Table 7.21: Panel Status Holding Register Bit Definitions

| Bit No. | Upper Byte | | | | | | | | Lower Byte | | | | | | | |
|----------|------------|----|----|----|----|----|---|---|------------|---|---|---|---|---|---------|-------|
| | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Bit Name | Not Used | | | | | | | | | | | | | | Silence | Reset |

Table 7.22: Panel Status Holding Register Addresses

| Start Address | End Address | Description |
|---------------|-------------|-------------------------------|
| 420001 | 420001 | Panel Status Holding Register |

7.23 Analog Values Input Registers

Analog values listed in [Table 7.23, “Input Register Analog Values”](#) are only available for 4–20 mA modules. Refer to [Table 7.23, “Input Register Analog Values”](#) for details regarding analog values.

Table 7.23: Input Register Analog Values

| Start Address | End Address | Analog Value (16 bits) |
|---------------|-------------|------------------------|
| 310001 | 310300 | L1M1–L1M300 |
| 310301 | 310600 | L2M1–L2M300 |
| 310601 | 310900 | L3M1–L3M300 |
| 310901 | 311200 | L4M1–L4M300 |
| 311201 | 311500 | L5M1–L5M300 |
| 311501 | 311800 | L6M1–L6M300 |
| 311801 | 312100 | L7M1–L7M300 |
| 312101 | 312400 | L8M1–L8M300 |
| 312401 | 312700 | L9M1–L9M300 |
| 312701 | 313000 | L10M1–L10M300 |

7.23.1 Panel and System Troubles Holding Registers

One hundred 16-bit registers are reserved for panel troubles and one register is assigned as an overall panel trouble indicator as shown in [Table 7.24, “Panel and System Troubles Holding Register Addresses”](#).

Table 7.24: Panel and System Troubles Holding Register Addresses

| Start Address | End Address | Description |
|---------------|-------------|--|
| 460000 | 460000 | Panel Trouble Summary (Total number of Trouble bits set for the node) |
| 460001 | 460100 | Panel Troubles |

A single bit is reserved for each trouble in the system. The assignment of bits to trouble codes is shown in [Table 7.33: “System Troubles Register Map”](#).

7.23.2 Gateway Information Input Registers



NOTE: Information/debug values are used by the CLSS Gateway Unit ID only. All other nodes reject reads in this address range.

The CLSS Gateway records some status and configuration information for debugging and technical support purposes. This information is stored in some reserved gateway registers as outlined below.

- Gateway Modbus Address
- Gateway IP Address
- Gateway Version Number

Table 7.25: Gateway Information Input Register Addresses

| Start Address | End Address | Description |
|---------------|-------------|---|
| 360001 | 360100 | Information/Debug information |
| 320001 | 320015 | Node Status: 1 = On Line 0 = Off Line The CLSS Gateway tracks status of network nodes under Modbus feature monitoring. |
| 360016 | 360016 | Gateway major version number |
| 360017 | 360017 | Gateway minor version number |
| 360018 | 360018 | Gateway feature number |
| 360019 | 360019 | Gateway build number |

7.23.3 Node Status Details

Each nodes status is represented by a bit in a register. If the bit is set, the node is on line. Below table provides an example of how this is represented in a register.

Table 7.26: Node Status Example

| Addresses | Bit Number | | | | | | | | | | | | | | | |
|-----------|------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 320001 | N16 | N15 | N14 | N13 | N12 | N11 | N10 | N9 | N8 | N7 | N6 | N5 | N4 | N3 | N2 | N1 |
| 320002 | N32 | N31 | N30 | N29 | N28 | N27 | N26 | N25 | N24 | N23 | N22 | N21 | N20 | N19 | N18 | N17 |

7.24 Read Device Identification (0x2B/0x0E)

This function code allows reading the identification and additional information about the CLSS Gateway.

Table 7.27: Read Device Identification (0x2B/0x0E)

| Object ID | Object Name / Description | Value |
|-----------|---------------------------|------------------|
| 0x00 | VendorName | Notifier |
| 0x01 | ProductCode | 1 |
| 0x02 | MajorMinorRevision | V1.0 (Example) |
| 0x03 | VendorUrl | www.notifier.com |
| 0x04 | ProductName | Modbus Gateway |
| 0x05 | ModelName | Modbus Gateway |
| 0x06 | UserApplicationName | Modbus Gateway |
| 0x07 | MappingVersion | V1.0 (Example) |

7.25 Troubleshooting

7.25.1 What are some basic guidelines when installing a CLSS Gateway?

- Polling should be done slowly to start.
- Use Modscan® to debug the system rather than a more complicated client. Verify that registers are being updated as events happen on the NFN network/panel.
- Make sure gateway can be pinged from the same computer on which the client application is being installed.
- Check and double check the power supplies as well as all cabling.
- Make sure the client supports Unit IDs.
- Stop the client from sending a subsequent request until after it receives a response from the gateway.
- Make sure the client accepts all exception responses. Including OxA and OxB.
- Use Wireshark® to debug IP traffic.
- Be sure only one client is polling the gateway.
- Check the CLSS Gateway configuration tool and be sure that the Authorized Client IP address is set to **0.0.0.0**. If using the Authorized Client IP security feature, confirm that the address in the gateway matches the address in the Modbus client.

7.25.2 How fast can the Modbus client poll the gateway?

The polling rate is a function of several variables. Some issues that will determine the maximum poll rate are:

- The size of the NFN network that is being monitored.
- The number of points on the panels.
- The event activity on the NFN network/panel (i.e. VeriFire downloads).
- Requests for analog values are much slower than other requests
- If only a partial response from the gateway is seen in the Modbus client, try increasing the “response time out” value in the client to a larger value. If the value is set to 5 seconds or more, this should be adequate. The exact response time out will depend on IP network delays and routing. On a small IP network, the gateway responds to a read of 100 register in less than 1 second.

The gateway also has some processing overhead in order to do such things as maintain the registers.

7.25.3 How can I tell if the gateway is running?

- Ping the gateway from the computer on which the Modbus client is running.
- Use Wireshark to analyze the data on the IP network.
- Modscan was one tool that was used during development to test the gateway. It is designed primarily as a testing device for verification of correct protocol operation in new or existing systems.

7.25.4 How do I recover a lost password from the gateway?

If the password for the gateway is lost, programming changes cannot be made. In this situation, the gateway settings must be reset.

7.25.5 What is an “initialization read” for analog values?

This is the first read of up to 10 analog values from a 4–20 mA module. This first read tells the gateway that it should begin a polling routine for the analog values in this request. The first response from the initialization will usually be all zeros. Subsequent responses will have the actual values.

7.25.6 How many analog values can I read at a time?

Ten analog values can be read at one time. An initialization read must be performed.

7.25.7 Why do I get an exception code when trying to read an analog value?

There are several reasons why an exception code is received when requesting an analog value:

- The point from which an analog value is being requested is not a 4–20 mA analog input module.
- At least one of the points in the group of points from which an analog value is being requested is not a 4–20 mA analog input module.
- More than 10 analog values have been requested in a single request.

7.25.8 Why do I get all zeros when I read an analog value?

There are several reasons a zero reading from an FMM-4-20 Analog Input Module is received:

- The first read for an analog value from the gateway initializes the polling routine in the gateway to retrieve analog values from the NFN network. The first response will usually be all zeros. This is normal. The subsequent polls of an analog value for the same point or group of points will return actual values. As long as the same points continue to be polled at a rate faster than the Analog Poll Time Out, then the gateway will continue to poll the same points.
- The gateway does not actually take an analog value reading unless the module has reached the first threshold and therefore it will return a zero reading.
- If the client polls the gateway too quickly after the initialization poll then the gateway may still return zeros.
- If the client polls the analog values slower than the Analog Poll Time Out, then the gateway may return all zeros.

7.26 What is the “Analog Value Polling Time Out”?

This is how long a gateway will continue to poll analog points after the last client read request of the points. As long as the client makes analog reads of the same points faster than the Analog Value Polling Time then the gateway will continue to poll these points. If the client polls slower than the Analog Value Polling Time then the gateway may return readings of zero because this will be considered an initialization read.

7.27 Conversion to Modbus RTU

CLSS Gateway (acting as a Modbus slave) interfaces with a Modbus master through Modbus TCP protocol. For a Modbus RTU master to interface with the CLSS Gateway, use Moxa MGate MB3180 and convert the Modbus TCP protocol to the Modbus RTU (Serial) protocol.

7.27.1 Hardware Configuration

Refer to the *Moxa MGate MB3180 Quick Installation Guide* for hardware configuration of the MB3180.

7.27.2 Software Configuration

Configure the CLSS Gateway as a node in the NFN network with a node number.



CAUTION: ENSURE THAT THE NFN NETWORK CONFIGURATIONS ARE UNCHANGED.

Refer to the *NOTI•FIRE•NET™ Network Systems Interface Manual (P/N 51584)* or the *High Speed NOTI•FIRE•NET™ Instruction Manual (P/N 54013)* for details about network configuration.

When configuring the network, refer to the settings specified in [Table 7.28: "MGate MB3180 Configuration Settings"](#). Settings not specified should be tailored to your network requirements. Refer to the *MGate MB3000 Modbus Gateway User's Manual* for details.

1. Connect the MB3180 to a configuration computer through an Ethernet cable as shown in [Figure 7.7](#).

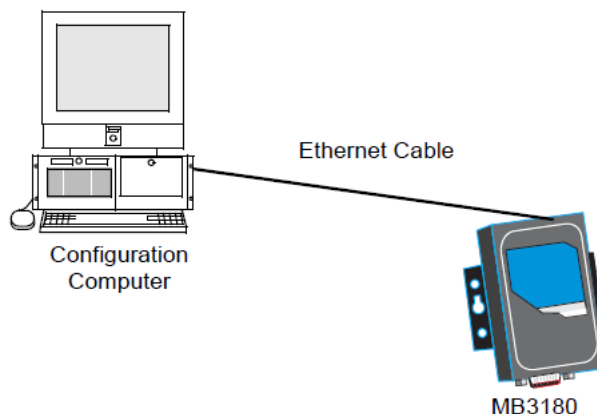


Figure 7.7: Connect a Configuration Computer

2. Run the *MGate Manager* installation software (`MGM_SETUP_VERX.X_BUILD_XXXXXXX.EXE`) found on the Software CD shipped with the MGate MB3180.
3. Wait for the installation to complete.
4. Run *MGate Manager*.
5. Power up the MB3180.
6. Ensure that the **Ready** and **Ethernet** lights are ON.
7. Configure the MB3180 for the network.
8. Wait for the configuration to complete.
9. Click **OK**.
10. Click **Exit**.

Table 7.28: MGate MB3180 Configuration Settings

| Tab | Setting |
|--------------|---|
| Mode | RTU Master Mode |
| Slave ID Map | The MGate MB3180 accepts the Modbus Unit ID as a virtual slave ID and monitors devices with these virtual slave IDs. By default, the CLSS Gateway assigns a Modbus Unit ID to each node on the NFN network. The ID is equal to node number of the node. They can be changed, but should be within 1 to 99. Refer to the 7.17 "To Configure the Modbus Settings" section for more information about changing a Modbus Unit ID. |
| Modbus | Initial Delay: 0 ms Response Time-out: 1000 ms |

7.27.3 Connecting the Moxa MGate MB3180 Interface



NOTE: The configuration used must have the approval of the AHJ (Authority Having Jurisdiction).

1. Connect the RTU master to the Serial port (RS-232, RS-485, or RS-422) of MB3180.
2. Connect the MB3180 to the CLSS Gateway.

Figures 7.8 and 7.9 show possible configurations for connecting the CLSS Gateway to the Moxa interface.

3. Power up the system.

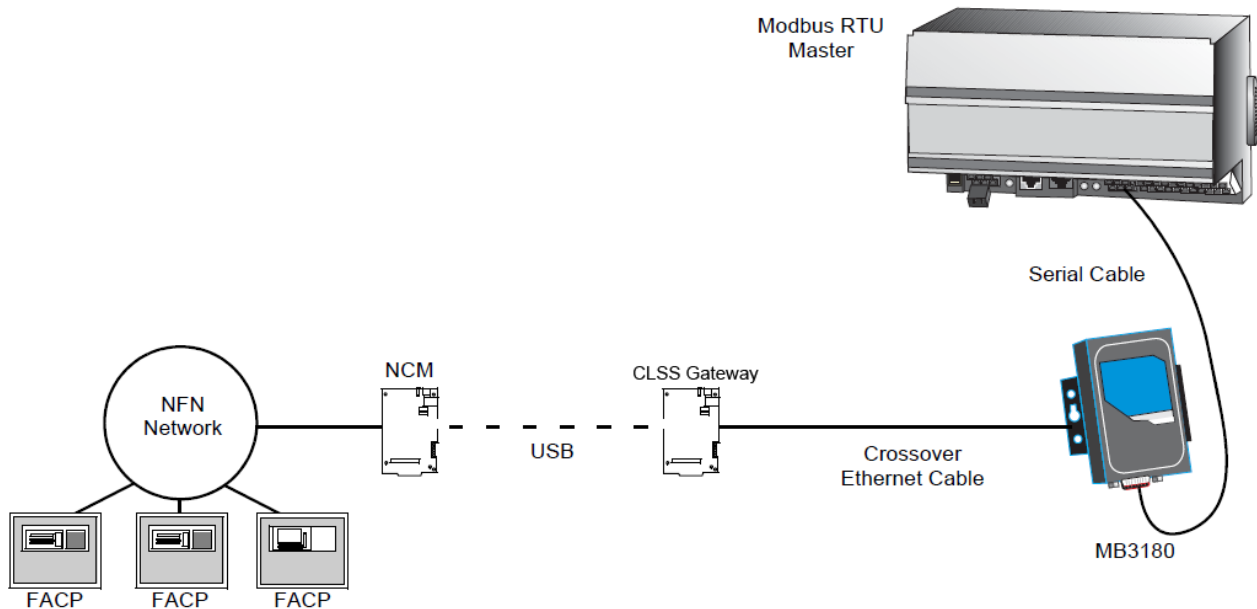


Figure 7.8: Connection Through Crossover Ethernet Cable

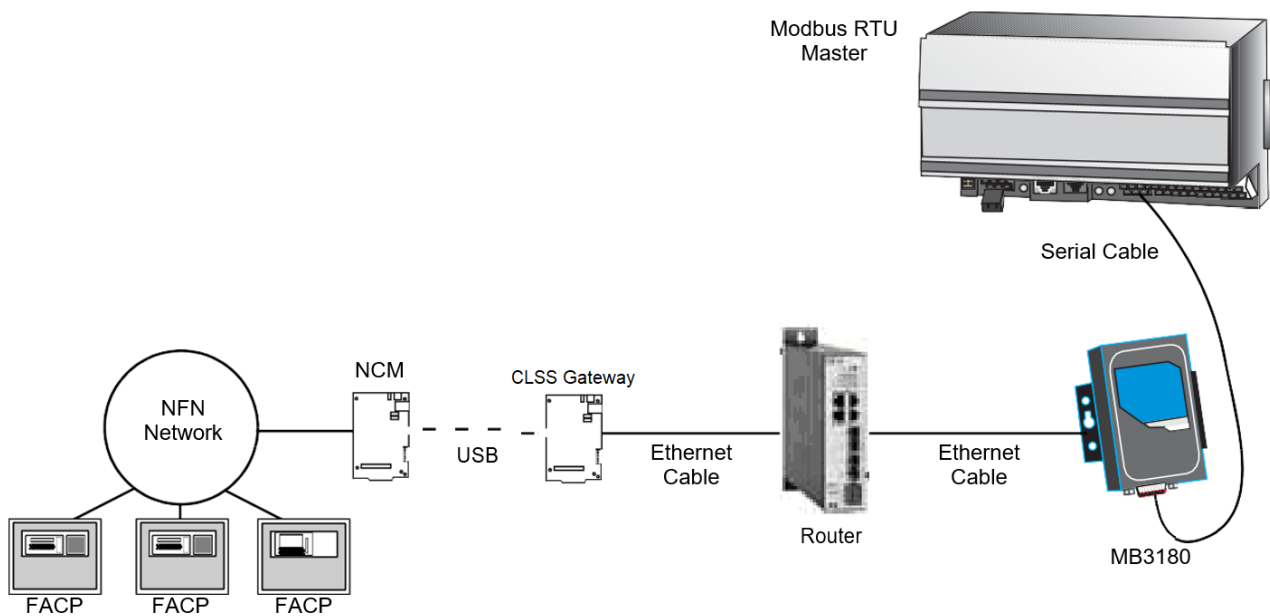


Figure 7.9: Connection Through a Router

7.28 System Trouble

For information about system trouble information stored in holding registers, refer to [7.23.1 "Panel and System Troubles Holding Registers"](#).

7.29 Exception Responses

If a Modbus master device sends an invalid command or attempts to read an invalid holding register, an exception response is generated. The exception response follows the standard packet format. The high order bit of the function code in an exception response is 1. The data field of an exception response contains the exception error code. The table describes the exception codes supported and the possible causes.

Table 7.29: Exception Codes


| Exception Code | Conditions | Exception Name |
|----------------|--|-----------------------|
| 0x01 | Protocol Identifier in Modbus packet does not match Modbus protocol. Protocol Identifier in Modbus should always be "0". Function code sent by the client is not supported by the CLSS Gateway or the FACP. A Control command was sent to the gateway. Contact customer service. | Illegal function |
| 0x02 | Register address range specified by the client is not supported by the FACP. Register address range requested is valid but the device (e.g. Detector, Module, Zone, etc.) is not present in the specified FACP. Analog Value is requested from a register which is not associated with a 4–20 mA device. | Illegal data address |
| 0x03 | Number of registers requested exceeds the maximum allowed limit. The maximum number of registers that a client can read at one time is 100. The exception to this is for analog values where the maximum number of registers a client can read at one time is 10. Invalid Data written to the register when sending commands. | Illegal data value |
| 0x0A | Unit ID specified in the request packet is not configured for monitoring. | Gateway path failed |
| 0x0B | FACP is off line or there is a communication problem on the panel and/or NFN. | Gateway target failed |

7.30 CLSS Gateway Active Event Code

All events are mapped into Modbus event categories which are stored in the Modbus register.

Table 7.30: Event Type Categories

| Event | Modbus Register Value |
|--|-----------------------|
| No Active Status (see note) | 00H |
| Mass Notification Alarm, High Priority | 05H |
| Fire Alarm | 10H |
| Security Alarm (Life) | 11H |
| Critical Process Alarm (Life) | 12H |
| Medical Emergency (Life) | 13H |
| CO Alarm | 14H |
| Mass Notification Alarm, Low Priority | 15H |
| Security Alarm (Property) | 20H |
| Critical Process (Property) | 21H |
| Mass Notification Supervisory, High Priority | 25H |
| Supervisory Signal (Guard's Tour) | 30H |
| Supervisory Signal (Equipment) | 40H |
| Mass Notification Supervisory, Low Priority | 45H |
| Disabled Alarm (AFP2800 Panel Only) | 52H |
| Disabled Active (AFP2800 Panel Only) | 55H |
| Non-Fire Activation | 71H |
| Non-Fire Activation (no acknowledgment required) | 72H |
| CO Alarm & Fire Alarm | EAH |
| CO Supervisory | EBH |
| CO Supervisory & Photo Supervisory | ECH |
| CO Supervisory & Fire Alarm | EDH |
| CO Alarm & Photo Supervisory | EEH |
| Device Not Present | FFH |

 **NOTE:** Multiple states are possible for a device. For example, a device connected to a Fire Alarm Control Panel may be both Active and Disabled. Also, a device may be in the Trouble and Fire Alarm states at one time.

“No Active Status” does not indicate the point/device is in a normal state. The holding register for the point or device contains more detail. For more information, refer to [7.22 "Register Mapping"](#).

7.31 Device Types

Device types are organized into the following categories:

- Detectors (1–50) - [Table 7.31: "Device Type Values – Detectors"](#)
- Modules (51–150) - [Table 7.32: "Device Type Values – Modules"](#)

Table 7.31: Device Type Values – Detectors

| Device Type | Value | Device Type | Value |
|-------------------------------|-------|-------------------------------|-------|
| Not Identified | 0000H | Wireless Smoke Photo Tracking | 0311H |
| Heat | 0100H | Smoke Laser Latching | 0400H |
| Heat (rate of rise) | 0101H | Smoke Laser Tracking | 0401H |
| Heat (fixed) | 0102H | Duct Smoke Laser Latching | 0402H |
| Heat (high heat) | 0103H | Duct Smoke Laser Tracking | 0403H |
| Wireless Heat | 0110H | Air Reference Laser | 0404H |
| Wireless Heat (rate of rise) | 0111H | Smoke (Harsh) | 0500H |
| Wireless Heat (fixed) | 0112H | Smoke (Beam) | 0501H |
| Wireless (high heat) | 0113H | Smoke Multi | 0600H |
| Smoke Ion Latching | 0200H | Smoke Acclimate | 0601H |
| Smoke Ion Tracking | 0201H | Wireless Smoke Multi | 0610H |
| Duct Smoke Ion Latching | 0202H | Wireless Smoke Acclimate | 0611H |
| Duct Smoke Ion Tracking | 0203H | CO Alarm | 0700H |
| Smoke Photo Latching | 0300H | Fire/CO | 0701H |
| Smoke Photo Tracking | 0301H | Photo/CO | 0702H |
| Duct Smoke Photo Latching | 0302H | CO/Photo/Thermal/IR | 0703H |
| Duct Smoke Photo Tracking | 0303H | Aspiration | 0801H |
| Smoke (Photo Flame) | 0304H | Aspir. Ref | 0802H |
| Wireless Smoke Photo Latching | 0310H | | |

Table 7.32: Device Type Values – Modules

| Device Type | Value | Device Type | Value |
|---------------------------------|-------|---------------------------------|-------|
| Not Identified | 0000H | Acknowledge Switch | 0041H |
| Heat Detection Circuit | 0001H | Wireless Acknowledge Switch | 0042H |
| Wireless Heat Detection Circuit | 0002H | All Call Page | 0043H |
| Conventional Smoke | 0003H | Drill Switch | 0044H |
| Wireless Conventional Smoke | 0004H | Wireless Drill Switch | 0045H |
| Smoke Detection | 0005H | Evacuate Switch | 0046H |
| Wireless Smoke Detection | 0006H | Wireless Evacuate Switch | 0047H |
| Monitor | 0010H | Signals Silence Switch | 0048H |
| Wireless Monitor | 0011H | Wireless Signals Silence Switch | 0049H |
| Pull Station | 0012H | Reset Switch | 004AH |
| Wireless Pull Station | 0013H | Wireless Reset Switch | 004BH |

| | | | |
|---|-------|---|-------|
| Monitor Tracking | 0014H | Fire Control | 0050H |
| Wireless Monitor Tracking | 0015H | Hazard | 0051H |
| Normally Closed Monitor | 0016H | Wireless Hazard | 0052H |
| Wireless Normally Closed Monitor | 0017H | Medical | 0053H |
| Normally Closed Monitor Tracking | 0018H | Wireless Medical | 0054H |
| Wireless Normally Closed Monitor Tracking | 0019H | Relay | 1002H |
| Disable | 001AH | Wireless Relay | 1003H |
| Wireless Disable | 001BH | Non-reset Control | 1004H |
| Waterflow | 0020H | Wireless Non-Reset Control | 1005H |
| Wireless Waterflow | 0021H | Bell Circuit | 1010H |
| Sprinkler System | 0022H | Strobe Circuit | 1011H |
| Access Monitor | 0030H | Horn Circuit | 1012H |
| Wireless Access Monitor | 0031H | Speaker Circuit | 1013H |
| Area Monitor | 0032H | Speaker | 1014H |
| Wireless Area Monitor | 0033H | Telephone | 1015H |
| Equipment Monitor | 0034H | Isolated Speaker | 1016H |
| Wireless Equipment Monitor | 0035H | Isolated Notification Appliance Circuit | 1017H |
| Hold Up | 0036H | Releasing Circuit | 1020H |
| Wireless Hold Up | 0037H | Releasing Circuit ULC | 1021H |
| Tamper | 0038H | Releasing Form C | 1022H |
| Wireless Tamper | 0039H | Releasing Bell | 1023H |
| Secure/Access | 003AH | Releasing Audible | 1024H |
| Telephone Page | 0040H | Instant Release | 1030H |
| Weather | 0055H | Alarms Pending | 1031H |
| Wireless Weather | 0056H | Control Notification Appliance Circuit | 1032H |
| Positive Alarm Sequence Inhibit Input | 0060H | General Alarm | 1033H |
| Abort Switch | 0061H | General Supervisory | 1034H |
| Manual Release | 0062H | General Trouble | 1035H |
| Manual Release Delay | 0063H | General Pending | 1036H |
| Second Shot | 0064H | Trouble Pending | 1037H |
| Audio System | 0070H | Form C Reset | 1038H |
| Power Supply | 0071H | Relay Feedback | 1040H |
| Wireless System | 0072H | Relay Form C Feedback | 1041H |
| Bi-Directional Amplifier/Distributed Antenna System | 0073H | Control Feedback | 1042H |
| Process Monitor | 0080H | ECS/MNS General | 1050H |
| Process Auto | 0081H | ECS/MNS Control | 1051H |
| 4-20mA sensor | 0090H | ECS/MNS Strobe | 1052H |
| Wireless 4-20mA sensor | 0091H | ECS/MNS Speaker | 1053H |
| Feedback | 00A0H | ECS/MNS Relay | 1054H |

| | | | |
|-------------------|-------|----------------|-------|
| Feedback Tracking | 00A1H | Auxiliary | 1060H |
| Hydrant | 00A2H | Door Holder | 1061H |
| Control | 1000H | AAM Sounder | 1062H |
| Wireless Control | 1001H | TYPE 5 Control | 1063H |

7.32 System Troubles Register Map

Table 7.33: System Troubles Register Map

| Register | Bit No. | System Trouble Name | Bit No. | System Trouble Name |
|----------|---------|---------------------------------|---------|---------------------|
| 460001 | 0 | GROUND FAULT | 8 | INTERNAL RAM ERROR |
| | 1 | AC FAIL | 9 | EXTERNAL RAM ERROR |
| | 2 | BATTERY | 10 | PROGRAM CORRUPTED |
| | 3 | STYLE 6 POS. LOOP 1 | 11 | NO DEV. INST ON L1 |
| | 4 | STYLE 6 POS. LOOP 2 | 12 | PANEL DOOR OPEN |
| | 5 | CORRUPT LOGIC EQUAT | 13 | AUXILIARY TROUBLE |
| | 6 | LCD80 SUPERVISORY | 14 | TERM. SUPERVISORY |
| | 7 | EPROM ERROR / FLASH IMAGE ERROR | 15 | ANNUN. 1 TROUBLE |
| 460002 | 0 | ANNUN. 1 NO ANSWER | 8 | ANNUN. 5 NO ANSWER |
| | 1 | ANNUN. 2 TROUBLE | 9 | ANNUN. 6 TROUBLE |
| | 2 | ANNUN. 2 NO ANSWER | 10 | ANNUN. 6 NO ANSWER |
| | 3 | ANNUN. 3 TROUBLE | 11 | ANNUN. 7 TROUBLE |
| | 4 | ANNUN. 3 NO ANSWER | 12 | ANNUN. 7 NO ANSWER |
| | 5 | ANNUN. 4 TROUBLE | 13 | ANNUN. 8 TROUBLE |
| | 6 | ANNUN. 4 NO ANSWER | 14 | ANNUN. 8 NO ANSWER |
| | 7 | ANNUN. 5 TROUBLE | 15 | ANNUN. 9 TROUBLE |
| 460003 | 0 | ANNUN. 9 NO ANSWER | 8 | ANNUN.13 NO ANSWER |
| | 1 | ANNUN.10 TROUBLE | 9 | ANNUN.14 TROUBLE |
| | 2 | ANNUN.10 NO ANSWER | 10 | ANNUN.14 NO ANSWER |
| | 3 | ANNUN.11 TROUBLE | 11 | ANNUN.15 TROUBLE |
| | 4 | ANNUN.11 NO ANSWER | 12 | ANNUN.15 NO ANSWER |
| | 5 | ANNUN.12 TROUBLE | 13 | ANNUN.16 TROUBLE |
| | 6 | ANNUN.12 NO ANSWER | 14 | ANNUN.16 NO ANSWER |
| | 7 | ANNUN.13 TROUBLE | 15 | ANNUN.17 TROUBLE |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|---------------------|----|----------------------|
| 460004 | 0 | ANNUN.17 NO ANSWER | 8 | ANNUN.21 NO ANSWER |
| | 1 | ANNUN.18 TROUBLE | 9 | ANNUN.22 TROUBLE |
| | 2 | ANNUN.18 NO ANSWER | 10 | ANNUN.22 NO ANSWER |
| | 3 | ANNUN.19 TROUBLE | 11 | ANNUN.23 TROUBLE |
| | 4 | ANNUN.19 NO ANSWER | 12 | ANNUN.23 NO ANSWER |
| | 5 | ANNUN.20 TROUBLE | 13 | ANNUN.24 TROUBLE |
| | 6 | ANNUN.20 NO ANSWER | 14 | ANNUN.24 NO ANSWER |
| | 7 | ANNUN.21 TROUBLE | 15 | ANNUN.25 TROUBLE |
| 460005 | 0 | ANNUN.25 NO ANSWER | 8 | ANNUN.29 NO ANSWER |
| | 1 | ANNUN.26 TROUBLE | 9 | ANNUN.30 TROUBLE |
| | 2 | ANNUN.26 NO ANSWER | 10 | ANNUN.30 NO ANSWER |
| | 3 | ANNUN.27 TROUBLE | 11 | ANNUN.31 TROUBLE |
| | 4 | ANNUN.27 NO ANSWER | 12 | ANNUN.31 NO ANSWER |
| | 5 | ANNUN.28 TROUBLE | 13 | ANNUN.32 TROUBLE |
| | 6 | ANNUN.28 NO ANSWER | 14 | ANNUN.32 NO ANSWER |
| | 7 | ANNUN.29 TROUBLE | 15 | NETWORK FAIL PORT A |
| 460006 | 0 | NETWORK FAIL PORT B | 8 | UDACT TROUBLE |
| | 1 | NETWORK FAILURE | 9 | UDACT NO ANSWER |
| | 2 | ADV WALK TEST | 10 | PROG MODE ACTIVATED |
| | 3 | CHARGER FAIL | 11 | LOADING ..NO SERVICE |
| | 4 | GROUND FAULT LOOP 2 | 12 | BASIC WALK TEST |
| | 5 | STYLE 6 NEG. LOOP 1 | 13 | NFPA 24HR REMINDER |
| | 6 | STYLE 6 NEG. LOOP 2 | 14 | NVRAM BATT TROUBLE |
| | 7 | GROUND FAULT LOOP 1 | 15 | (Reserved) |
| 460007 | 0 | Reserved | 8 | OPTION MODULE |
| | 1 | Reserved | 9 | STYLE 6 ON LOOP 3 |
| | 2 | Reserved | 10 | AVPS. TROUBLE |
| | 3 | Reserved | 11 | NAM CCBE PROG. LOST |
| | 4 | Reserved | 12 | MAN. EVAC INITIATED |
| | 5 | Reserved | 13 | MAN. EVAC RECEIVED |
| | 6 | Reserved | 14 | (Reserved) |
| | 7 | Reserved | 15 | (Reserved) |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|--------------------|----|--------------------|
| 460008 | 0 | ANNUN.33 TROUBLE | 8 | ANNUN.37 TROUBLE |
| | 1 | ANNUN.33 NO ANSWER | 9 | ANNUN.37 NO ANSWER |
| | 2 | ANNUN.34 TROUBLE | 10 | ANNUN.38 TROUBLE |
| | 3 | ANNUN.34 NO ANSWER | 11 | ANNUN.38 NO ANSWER |
| | 4 | ANNUN.35 TROUBLE | 12 | ANNUN.39 TROUBLE |
| | 5 | ANNUN.35 NO ANSWER | 13 | ANNUN.39 NO ANSWER |
| | 6 | ANNUN.36 TROUBLE | 14 | ANNUN.40 TROUBLE |
| | 7 | ANNUN.36 NO ANSWER | 15 | ANNUN.40 NO ANSWER |
| 460009 | 0 | ANNUN.41 TROUBLE | 8 | ANNUN.45 TROUBLE |
| | 1 | ANNUN.41 NO ANSWER | 9 | ANNUN.45 NO ANSWER |
| | 2 | ANNUN.42 TROUBLE | 10 | ANNUN.46 TROUBLE |
| | 3 | ANNUN.42 NO ANSWER | 11 | ANNUN.46 NO ANSWER |
| | 4 | ANNUN.43 TROUBLE | 12 | ANNUN.47 TROUBLE |
| | 5 | ANNUN.43 NO ANSWER | 13 | ANNUN.47 NO ANSWER |
| | 6 | ANNUN.44 TROUBLE | 14 | ANNUN.48 TROUBLE |
| | 7 | ANNUN.44 NO ANSWER | 15 | ANNUN.48 NO ANSWER |
| 460010 | 0 | ANNUN.49 TROUBLE | 8 | ANNUN.53 TROUBLE |
| | 1 | ANNUN.49 NO ANSWER | 9 | ANNUN.53 NO ANSWER |
| | 2 | ANNUN.50 TROUBLE | 10 | ANNUN.54 TROUBLE |
| | 3 | ANNUN.50 NO ANSWER | 11 | ANNUN.54 NO ANSWER |
| | 4 | ANNUN.51 TROUBLE | 12 | ANNUN.55 TROUBLE |
| | 5 | ANNUN.51 NO ANSWER | 13 | ANNUN.55 NO ANSWER |
| | 6 | ANNUN.52 TROUBLE | 14 | ANNUN.56 TROUBLE |
| | 7 | ANNUN.52 NO ANSWER | 15 | ANNUN.56 NO ANSWER |
| 460011 | 0 | ANNUN.57 TROUBLE | 8 | ANNUN.61 TROUBLE |
| | 1 | ANNUN.57 NO ANSWER | 9 | ANNUN.61 NO ANSWER |
| | 2 | ANNUN.58 TROUBLE | 10 | ANNUN.62 TROUBLE |
| | 3 | ANNUN.58 NO ANSWER | 11 | ANNUN.62 NO ANSWER |
| | 4 | ANNUN.59 TROUBLE | 12 | ANNUN.63 TROUBLE |
| | 5 | ANNUN.59 NO ANSWER | 13 | ANNUN.63 NO ANSWER |
| | 6 | ANNUN.60 TROUBLE | 14 | ANNUN.64 TROUBLE |
| | 7 | ANNUN.60 NO ANSWER | 15 | ANNUN.64 NO ANSWER |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|----------------------------------|----|---|
| 460012 | 0 | GROUND FAULT LOOP 3 | 8 | STYLE 6 NEG. LOOP 3 |
| | 1 | GROUND FAULT LOOP 4 | 9 | STYLE 6 NEG. LOOP 4 |
| | 2 | GROUND FAULT LOOP 5 | 10 | STYLE 6 NEG. LOOP 5 |
| | 3 | GROUND FAULT LOOP 6 | 11 | STYLE 6 NEG. LOOP 6 |
| | 4 | GROUND FAULT LOOP 7 | 12 | STYLE 6 NEG. LOOP 7 |
| | 5 | GROUND FAULT LOOP 8 | 13 | STYLE 6 NEG. LOOP 8 |
| | 6 | GROUND FAULT LOOP 9 | 14 | STYLE 6 NEG. LOOP 9 |
| | 7 | GROUND FAULT LOOP 10 | 15 | STYLE 6 NEG. LOOP 10 |
| 460013 | 0 | STYLE 6 POS. LOOP 3 | 8 | PRINTER SUPERVISORY |
| | 1 | STYLE 6 POS. LOOP 4 | 9 | BUZZER SUPERVISORY |
| | 2 | STYLE 6 POS. LOOP 5 | 10 | CRT SUPERVISORY |
| | 3 | STYLE 6 POS. LOOP 6 | 11 | PRINT QUEUE FULL |
| | 4 | STYLE 6 POS. LOOP 7 | 12 | MEMORY LOSS |
| | 5 | STYLE 6 POS. LOOP 8 | 13 | PRINTER COVER OPEN |
| | 6 | STYLE 6 POS. LOOP 9 | 14 | PRINTER PAPER OUT |
| | 7 | STYLE 6 POS. LOOP 10 | 15 | PRINTER OFF LINE |
| 460014 | 0 | Workstation Fan Failure | 8 | STYLE 4 SHORT A LOOP 3 |
| | 1 | UPS Failure | 9 | STYLE 4 SHORT B LOOP 3 |
| | 2 | MANUAL MODE ENTERED | 10 | STYLE 4 SHORT A LOOP 4 |
| | 3 | NCM COMM LOSS | 11 | STYLE 4 SHORT B LOOP 4 |
| | 4 | STYLE 4 SHORT A LOOP 1 | 12 | STYLE 4 SHORT A LOOP 5 |
| | 5 | STYLE 4 SHORT B LOOP 1 | 13 | STYLE 4 SHORT B LOOP 5 |
| | 6 | STYLE 4 SHORT A LOOP 2 | 14 | STYLE 4 SHORT A LOOP 6 |
| | 7 | STYLE 4 SHORT B LOOP 2 | 15 | STYLE 4 SHORT B LOOP 6 |
| 460015 | 0 | STYLE 4 SHORT A LOOP 7 | 8 | GENERAL PS FAULT / POWER SUPPLY TROUBLE |
| | 1 | STYLE 4 SHORT B LOOP 7 | 9 | STYLE 6 SHORT LOOP 1 |
| | 2 | STYLE 4 SHORT A LOOP 8 | 10 | STYLE 6 SHORT LOOP 2 |
| | 3 | STYLE 4 SHORT B LOOP 8 | 11 | STYLE 6 SHORT LOOP 3 |
| | 4 | STYLE 4 SHORT A LOOP 9 | 12 | STYLE 6 SHORT LOOP 4 |
| | 5 | STYLE 4 SHORT B LOOP 9 | 13 | STYLE 6 SHORT LOOP 5 |
| | 6 | STYLE 4 SHORT A LOOP 10 | 14 | STYLE 6 SHORT LOOP 6 |
| | 7 | STYLE 4 SHORT B LOOP 10 | 15 | STYLE 6 SHORT LOOP 7 |
| 460016 | 0 | STYLE 6 SHORT LOOP 8 | 8 | TM4 NO ANSWER |
| | 1 | STYLE 6 SHORT LOOP 9 | 9 | TM4 DISABLED |
| | 2 | STYLE 6 SHORT LOOP 10 | 10 | SELF TEST FAILED |
| | 3 | NODE xxx COMMUNICATIONS FAILURE | 11 | NETWORK INCOMPATIBILITY |
| | 4 | NCM PIEZO BATTERY FAILURE | 12 | WORKSTATION FAILURE |
| | 5 | DVC COMM LOSS | 13 | NETWORK MAPPING LIMIT EXCEEDED |
| | 6 | POWER SUPPLY CABLE NOT CONNECTED | 14 | INVALID NODE TYPE |
| | 7 | TM4 TROUBLE | 15 | DISPLAY NODE LIMIT EXCEEDED |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|----------------------|----|----------------------|
| 460017 | 0 | ANNUN. 65 TROUBLE | 8 | ANNUN. 69 TROUBLE |
| | 1 | ANNUN. 65 NO ANSWER | 9 | ANNUN. 69 NO ANSWER |
| | 2 | ANNUN. 66 TROUBLE | 10 | ANNUN. 70 TROUBLE |
| | 3 | ANNUN. 66 NO ANSWER | 11 | ANNUN. 70 NO ANSWER |
| | 4 | ANNUN. 67 TROUBLE | 12 | ANNUN. 71 TROUBLE |
| | 5 | ANNUN. 67 NO ANSWER | 13 | ANNUN. 71 NO ANSWER |
| | 6 | ANNUN. 68 TROUBLE | 14 | ANNUN. 72 TROUBLE |
| | 7 | ANNUN. 68 NO ANSWER | 15 | ANNUN. 72 NO ANSWER |
| 460018 | 0 | ANNUN. 73 TROUBLE | 8 | ANNUN. 77 TROUBLE |
| | 1 | ANNUN. 73 NO ANSWER | 9 | ANNUN. 77 NO ANSWER |
| | 2 | ANNUN. 74 TROUBLE | 10 | ANNUN. 78 TROUBLE |
| | 3 | ANNUN. 74 NO ANSWER | 11 | ANNUN. 78 NO ANSWER |
| | 4 | ANNUN. 75 TROUBLE | 12 | ANNUN. 79 TROUBLE |
| | 5 | ANNUN. 75 NO ANSWER | 13 | ANNUN. 79 NO ANSWER |
| | 6 | ANNUN. 76 TROUBLE | 14 | ANNUN. 80 TROUBLE |
| | 7 | ANNUN. 76 NO ANSWER | 15 | ANNUN. 80 NO ANSWER |
| 460019 | 0 | ANNUN. 81 TROUBLE | 8 | ANNUN. 85 TROUBLE |
| | 1 | ANNUN. 81 NO ANSWER | 9 | ANNUN. 85 NO ANSWER |
| | 2 | ANNUN. 82 TROUBLE | 10 | ANNUN. 86 TROUBLE |
| | 3 | ANNUN. 82 NO ANSWER | 11 | ANNUN. 86 NO ANSWER |
| | 4 | ANNUN. 83 TROUBLE | 12 | ANNUN. 87 TROUBLE |
| | 5 | ANNUN. 83 NO ANSWER | 13 | ANNUN. 87 NO ANSWER |
| | 6 | ANNUN. 84 TROUBLE | 14 | ANNUN. 88 TROUBLE |
| | 7 | ANNUN. 84 NO ANSWER | 15 | ANNUN. 88 NO ANSWER |
| 460020 | 0 | ANNUN. 89 TROUBLE | 8 | ANNUN. 93 TROUBLE |
| | 1 | ANNUN. 89 NO ANSWER | 9 | ANNUN. 93 NO ANSWER |
| | 2 | ANNUN. 90 TROUBLE | 10 | ANNUN. 94 TROUBLE |
| | 3 | ANNUN. 90 NO ANSWER | 11 | ANNUN. 94 NO ANSWER |
| | 4 | ANNUN. 91 TROUBLE | 12 | ANNUN. 95 TROUBLE |
| | 5 | ANNUN. 91 NO ANSWER | 13 | ANNUN. 95 NO ANSWER |
| | 6 | ANNUN. 92 TROUBLE | 14 | ANNUN. 96 TROUBLE |
| | 7 | ANNUN. 92 NO ANSWER | 15 | ANNUN. 96 NO ANSWER |
| 460021 | 0 | ANNUN. 97 TROUBLE | 8 | ANNUN. 101 TROUBLE |
| | 1 | ANNUN. 97 NO ANSWER | 9 | ANNUN. 101 NO ANSWER |
| | 2 | ANNUN. 98 TROUBLE | 10 | ANNUN. 102 TROUBLE |
| | 3 | ANNUN. 98 NO ANSWER | 11 | ANNUN. 102 NO ANSWER |
| | 4 | ANNUN. 99 TROUBLE | 12 | ANNUN. 103 TROUBLE |
| | 5 | ANNUN. 99 NO ANSWER | 13 | ANNUN. 103 NO ANSWER |
| | 6 | ANNUN. 100 TROUBLE | 14 | ANNUN. 104 TROUBLE |
| | 7 | ANNUN. 100 NO ANSWER | 15 | ANNUN. 104 NO ANSWER |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|-----------------------------|----|-----------------------------|
| 460022 | 0 | ANNUN. 105 TROUBLE | 8 | ANNUN. 109 TROUBLE |
| | 1 | ANNUN. 105 NO ANSWER | 9 | ANNUN. 109 NO ANSWER |
| | 2 | ANNUN. 106 TROUBLE | 10 | ANNUN. 110 TROUBLE |
| | 3 | ANNUN. 106 NO ANSWER | 11 | ANNUN. 110 NO ANSWER |
| | 4 | ANNUN. 107 TROUBLE | 12 | ANNUN. 111 TROUBLE |
| | 5 | ANNUN. 107 NO ANSWER | 13 | ANNUN. 111 NO ANSWER |
| | 6 | ANNUN. 108 TROUBLE | 14 | ANNUN. 112 TROUBLE |
| | 7 | ANNUN. 108 NO ANSWER | 15 | ANNUN. 112 NO ANSWER |
| 460023 | 0 | ANNUN. 113 TROUBLE | 8 | ANNUN. 117 TROUBLE |
| | 1 | ANNUN. 113 NO ANSWER | 9 | ANNUN. 117 NO ANSWER |
| | 2 | ANNUN. 114 TROUBLE | 10 | ANNUN. 118 TROUBLE |
| | 3 | ANNUN. 114 NO ANSWER | 11 | ANNUN. 118 NO ANSWER |
| | 4 | ANNUN. 115 TROUBLE | 12 | ANNUN. 119 TROUBLE |
| | 5 | ANNUN. 115 NO ANSWER | 13 | ANNUN. 119 NO ANSWER |
| | 6 | ANNUN. 116 TROUBLE | 14 | ANNUN. 120 TROUBLE |
| | 7 | ANNUN. 116 NO ANSWER | 15 | ANNUN. 120 NO ANSWER |
| 460024 | 0 | ANNUN. 121 TROUBLE | 8 | ANNUN. 125 TROUBLE |
| | 1 | ANNUN. 121 NO ANSWER | 9 | ANNUN. 125 NO ANSWER |
| | 2 | ANNUN. 122 TROUBLE | 10 | ANNUN. 126 TROUBLE |
| | 3 | ANNUN. 122 NO ANSWER | 11 | ANNUN. 126 NO ANSWER |
| | 4 | ANNUN. 123 TROUBLE | 12 | ANNUN. 127 TROUBLE |
| | 5 | ANNUN. 123 NO ANSWER | 13 | ANNUN. 127 NO ANSWER |
| | 6 | ANNUN. 124 TROUBLE | 14 | ANNUN. 128 TROUBLE |
| | 7 | ANNUN. 124 NO ANSWER | 15 | ANNUN. 128 NO ANSWER |
| 460025 | 0 | REMOTE DISPLAY 1 TROUBLE | 8 | REMOTE DISPLAY 5 TROUBLE |
| | 1 | REMOTE DISPLAY 1 NO ANSWER | 9 | REMOTE DISPLAY 5 NO ANSWER |
| | 2 | REMOTE DISPLAY 2 TROUBLE | 10 | REMOTE DISPLAY 6 TROUBLE |
| | 3 | REMOTE DISPLAY 2 NO ANSWER | 11 | REMOTE DISPLAY 6 NO ANSWER |
| | 4 | REMOTE DISPLAY 3 TROUBLE | 12 | REMOTE DISPLAY 7 TROUBLE |
| | 5 | REMOTE DISPLAY 3 NO ANSWER | 13 | REMOTE DISPLAY 7 NO ANSWER |
| | 6 | REMOTE DISPLAY 4 TROUBLE | 14 | REMOTE DISPLAY 8 TROUBLE |
| | 7 | REMOTE DISPLAY 4 NO ANSWER | 15 | REMOTE DISPLAY 8 NO ANSWER |
| 460026 | 0 | REMOTE DISPLAY 9 TROUBLE | 8 | REMOTE DISPLAY 13 TROUBLE |
| | 1 | REMOTE DISPLAY 9 NO ANSWER | 9 | REMOTE DISPLAY 13 NO ANSWER |
| | 2 | REMOTE DISPLAY 10 TROUBLE | 10 | REMOTE DISPLAY 14 TROUBLE |
| | 3 | REMOTE DISPLAY 10 NO ANSWER | 11 | REMOTE DISPLAY 14 NO ANSWER |
| | 4 | REMOTE DISPLAY 11 TROUBLE | 12 | REMOTE DISPLAY 15 TROUBLE |
| | 5 | REMOTE DISPLAY 11 NO ANSWER | 13 | REMOTE DISPLAY 15 NO ANSWER |
| | 6 | REMOTE DISPLAY 12 TROUBLE | 14 | REMOTE DISPLAY 16 TROUBLE |
| | 7 | REMOTE DISPLAY 12 NO ANSWER | 15 | REMOTE DISPLAY 16 NO ANSWER |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|-----------------------------|----|-----------------------------|
| 460027 | 0 | REMOTE DISPLAY 17 TROUBLE | 8 | REMOTE DISPLAY 21 TROUBLE |
| | 1 | REMOTE DISPLAY 17 NO ANSWER | 9 | REMOTE DISPLAY 21 NO ANSWER |
| | 2 | REMOTE DISPLAY 18 TROUBLE | 10 | REMOTE DISPLAY 22 TROUBLE |
| | 3 | REMOTE DISPLAY 18 NO ANSWER | 11 | REMOTE DISPLAY 22 NO ANSWER |
| | 4 | REMOTE DISPLAY 19 TROUBLE | 12 | REMOTE DISPLAY 23 TROUBLE |
| | 5 | REMOTE DISPLAY 19 NO ANSWER | 13 | REMOTE DISPLAY 23 NO ANSWER |
| | 6 | REMOTE DISPLAY 20 TROUBLE | 14 | REMOTE DISPLAY 24 TROUBLE |
| | 7 | REMOTE DISPLAY 20 NO ANSWER | 15 | REMOTE DISPLAY 24 NO ANSWER |
| 460028 | 0 | REMOTE DISPLAY 25 TROUBLE | 8 | REMOTE DISPLAY 29 TROUBLE |
| | 1 | REMOTE DISPLAY 25 NO ANSWER | 9 | REMOTE DISPLAY 29 NO ANSWER |
| | 2 | REMOTE DISPLAY 26 TROUBLE | 10 | REMOTE DISPLAY 30 TROUBLE |
| | 3 | REMOTE DISPLAY 26 NO ANSWER | 11 | REMOTE DISPLAY 30 NO ANSWER |
| | 4 | REMOTE DISPLAY 27 TROUBLE | 12 | REMOTE DISPLAY 31 TROUBLE |
| | 5 | REMOTE DISPLAY 27 NO ANSWER | 13 | REMOTE DISPLAY 31 NO ANSWER |
| | 6 | REMOTE DISPLAY 28 TROUBLE | 14 | REMOTE DISPLAY 32 TROUBLE |
| | 7 | REMOTE DISPLAY 28 NO ANSWER | 15 | REMOTE DISPLAY 32 NO ANSWER |
| 460029 | 0 | SYSTEM INITIALIZATION | 8 | Reserved |
| | 1 | POWER SUPPLY COMM FAILURE | 9 | Reserved |
| | 2 | Reserved | 10 | Reserved |
| | 3 | Reserved | 11 | Reserved |
| | 4 | Reserved | 12 | Reserved |
| | 5 | Reserved | 13 | Reserved |
| | 6 | Reserved | 14 | Reserved |
| | 7 | Reserved | 15 | Reserved |
| 460030 | 0 | Reserved | 8 | Reserved |
| | 1 | Reserved | 9 | Reserved |
| | 2 | Reserved | 10 | Reserved |
| | 3 | Reserved | 11 | Reserved |
| | 4 | Reserved | 12 | Reserved |
| | 5 | Reserved | 13 | Reserved |
| | 6 | Reserved | 14 | Reserved |
| | 7 | Reserved | 15 | Reserved |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|--|----|--|
| 460031 | 0 | Reserved | 8 | Reserved |
| | 1 | Reserved | 9 | Reserved |
| | 2 | Reserved | 10 | Reserved |
| | 3 | Reserved | 11 | Reserved |
| | 4 | Reserved | 12 | Reserved |
| | 5 | Reserved | 13 | Reserved |
| | 6 | Reserved | 14 | Reserved |
| | 7 | Reserved | 15 | Reserved |
| 460032 | 0 | Reserved | 8 | NO POWER SUPPLY INST |
| | 1 | Reserved | 9 | LOOP 1-2 COMM FAILURE |
| | 2 | LINK PROTECTOR PRIMARY STATUS | 10 | LOOP 3-4 COMM FAILURE |
| | 3 | LINK PROTECTOR SECONDARY STATUS | 11 | LOOP 5-6 COMM FAILURE |
| | 4 | LINK PROTECTOR NOT PRESENT | 12 | LOOP 7-8 COMM FAILURE |
| | 5 | EVENT BUFFER 80% FULL / HISTORY 80% FULL | 13 | LOOP 9-10 COMM FAILURE |
| | 6 | EBI STATUS | 14 | TEST PROGRAM UPDATE |
| | 7 | SOFTWARE MISMATCH | 15 | Reserved |
| 460033 | 0 | LOOP CONTINUITY TEST FAIL LOOP 1 | 8 | LOOP CONTINUITY TEST FAIL LOOP 9 |
| | 1 | LOOP CONTINUITY TEST FAIL LOOP 2 | 9 | LOOP CONTINUITY TEST FAIL LOOP 10 |
| | 2 | LOOP CONTINUITY TEST FAIL LOOP 3 | 10 | UNPROGRAMMED DEVICE ON LOOP 1 |
| | 3 | LOOP CONTINUITY TEST FAIL LOOP 4 | 11 | UNPROGRAMMED DEVICE ON LOOP 2 |
| | 4 | LOOP CONTINUITY TEST FAIL LOOP 5 | 12 | UNPROGRAMMED DEVICE ON LOOP 3 |
| | 5 | LOOP CONTINUITY TEST FAIL LOOP 6 | 13 | UNPROGRAMMED DEVICE ON LOOP 4 |
| | 6 | LOOP CONTINUITY TEST FAIL LOOP 7 | 14 | UNPROGRAMMED DEVICE ON LOOP 5 |
| | 7 | LOOP CONTINUITY TEST FAIL LOOP 8 | 15 | UNPROGRAMMED DEVICE ON LOOP 6 |
| 460034 | 0 | UNPROGRAMMED DEVICE ON LOOP 7 | 8 | IR ENABLED ON LOOP 5 |
| | 1 | UNPROGRAMMED DEVICE ON LOOP 8 | 9 | IR ENABLED ON LOOP 6 |
| | 2 | UNPROGRAMMED DEVICE ON LOOP 9 | 10 | IR ENABLED ON LOOP 7 |
| | 3 | UNPROGRAMMED DEVICE ON LOOP 10 | 11 | IR ENABLED ON LOOP 8 |
| | 4 | IR ENABLED ON LOOP 1 | 12 | IR ENABLED ON LOOP 9 |
| | 5 | IR ENABLED ON LOOP 2 | 13 | IR ENABLED ON LOOP 10 |
| | 6 | IR ENABLED ON LOOP 3 | 14 | TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 1 |
| | 7 | IR ENABLED ON LOOP 4 | 15 | TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 2 |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|---|----|---------------------------------|
| 460035 | 0 | TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 3 | 8 | TOO MANY DEVICES ON LOOP 1 |
| | 1 | TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 4 | 9 | TOO MANY DEVICES ON LOOP 2 |
| | 2 | TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 5 | 10 | TOO MANY DEVICES ON LOOP 3 |
| | 3 | TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 6 | 11 | TOO MANY DEVICES ON LOOP 4 |
| | 4 | TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 7 | 12 | TOO MANY DEVICES ON LOOP 5 |
| | 5 | TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 8 | 13 | TOO MANY DEVICES ON LOOP 6 |
| | 6 | TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 9 | 14 | TOO MANY DEVICES ON LOOP 7 |
| | 7 | TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 10 | 15 | TOO MANY DEVICES ON LOOP 8 |
| 460036 | 0 | TOO MANY DEVICES ON LOOP 9 | 8 | MISMATCHED LOOP TYPE ON LOOP 7 |
| | 1 | TOO MANY DEVICES ON LOOP 10 | 9 | MISMATCHED LOOP TYPE ON LOOP 8 |
| | 2 | MISMATCHED LOOP TYPE ON LOOP 1 | 10 | MISMATCHED LOOP TYPE ON LOOP 9 |
| | 3 | MISMATCHED LOOP TYPE ON LOOP 2 | 11 | MISMATCHED LOOP TYPE ON LOOP 10 |
| | 4 | MISMATCHED LOOP TYPE ON LOOP 3 | 12 | Ground Fault Port A |
| | 5 | MISMATCHED LOOP TYPE ON LOOP 4 | 13 | Ground Fault Port B |
| | 6 | MISMATCHED LOOP TYPE ON LOOP 5 | 14 | Amplifier Trouble |
| | 7 | MISMATCHED LOOP TYPE ON LOOP 6 | 15 | AUXIN Trouble |
| 460037 | 0 | DIGIN Trouble | 8 | ANALOG OUTPUT A TROUBLE |
| | 1 | FFT TROUBLE | 9 | ANALOG OUTPUT B TROUBLE |
| | 2 | REMOTE MIC Trouble | 10 | ANALOG OUTPUT C TROUBLE |
| | 3 | DAP Port A Failure | 11 | ANALOG OUTPUT D TROUBLE |
| | 4 | DAP Port B Failure | 12 | Reserved |
| | 5 | DAL No Answer / DAL DEVICE NO ANSWER | 13 | Reserved |
| | 6 | LOCAL MIC TROUBLE | 14 | AMPLIFIER LIMIT |
| | 7 | LOCAL PHONE TROUBLE | 15 | AMPLIFIER SUPERVISION |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|-----------------------------------|----|-----------------------------|
| 460038 | 0 | DAL ADDRESS CONFLICT | 8 | MAPPING IN PROGRESS LOOP 7 |
| | 1 | DEVICE SERVICING REQUIRED | 9 | MAPPING IN PROGRESS LOOP 8 |
| | 2 | MAPPING IN PROGRESS LOOP 1 | 10 | MAPPING IN PROGRESS LOOP 9 |
| | 3 | MAPPING IN PROGRESS LOOP 2 | 11 | MAPPING IN PROGRESS LOOP 10 |
| | 4 | MAPPING IN PROGRESS LOOP 3 | 12 | DATABASE CORRUPTED |
| | 5 | MAPPING IN PROGRESS LOOP 4 | 13 | AUDIO LIBRARY CORRUPTED |
| | 6 | MAPPING IN PROGRESS LOOP 5 | 14 | DATABASE INCOMPATIBLE |
| | 7 | MAPPING IN PROGRESS LOOP 6 | 15 | AUDIO LIBRARY INCOMPATIBLE |
| 460039 | 0 | DAL DOWNLOAD IN PROGRESS | 8 | PRIMARY AMP 1 TROUBLE |
| | 1 | FIRE VOICE TROUBLE | 9 | PRIMARY AMP 2 TROUBLE |
| | 2 | FIRE VOICE NO ANSWER | 10 | PRIMARY AMP 3 TROUBLE |
| | 3 | PHONE CHANNEL LIMIT EXCEEDED | 11 | PRIMARY AMP 4 TROUBLE |
| | 4 | NCM SMIFFER MODE ACTIVE | 12 | BACKUP AMP 1 TROUBLE |
| | 5 | LOCAL CONNECTION LIMIT EXCEEDED | 13 | BACKUP AMP 2 TROUBLE |
| | 6 | HARDWARE MISMATCH | 14 | BACKUP AMP 3 TROUBLE |
| | 7 | Reserved | 15 | BACKUP AMP 4 TROUBLE |
| 460040 | 0 | DSBUS 1 COMMFAL | 8 | PRIMARY AMP 2 LIMIT |
| | 1 | DSBUS 2 COMMFAL | 9 | PRIMARY AMP 3 LIMIT |
| | 2 | DSBUS 3 COMMFAL | 10 | PRIMARY AMP 4 LIMIT |
| | 3 | DSBUS 4 COMMFAL | 11 | BACKUP AMP 1 LIMIT |
| | 4 | AA TROUBLE BUS FAIL | 12 | BACKUP AMP 2 LIMIT |
| | 5 | NFN PAGING CHANNEL LIMIT EXCEEDED | 13 | BACKUP AMP 3 LIMIT |
| | 6 | BACKUP AMP LIMIT | 14 | BACKUP AMP 4 LIMIT |
| | 7 | PRIMARY AMP 1 LIMIT | 15 | PRIMARY AMP 1 OVERCURRENT |
| 460041 | 0 | PRIMARY AMP 2 OVERCURRENT | 8 | PRIMARY AMP 2 TRIP |
| | 1 | PRIMARY AMP 3 OVERCURRENT | 9 | PRIMARY AMP 3 TRIP |
| | 2 | PRIMARY AMP 4 OVERCURRENT | 10 | PRIMARY AMP 4 TRIP |
| | 3 | BACKUP AMP 1 OVERCURRENT | 11 | BACKUP AMP 1 TRIP |
| | 4 | BACKUP AMP 2 OVERCURRENT | 12 | BACKUP AMP 2 TRIP |
| | 5 | BACKUP AMP 3 OVERCURRENT | 13 | BACKUP AMP 3 TRIP |
| | 6 | BACKUP AMP 4 OVERCURRENT | 14 | BACKUP AMP 4 TRIP |
| | 7 | PRIMARY AMP 1 TRIP | 15 | DSBUS 1 AC FAIL |
| 460042 | 0 | DSBUS 2 AC FAIL | 8 | DSBUS 2 LOW BATT |
| | 1 | DSBUS 3 AC FAIL | 9 | DSBUS 3 LOW BATT |
| | 2 | DSBUS 4 AC FAIL | 10 | DSBUS 4 LOW BATT |
| | 3 | DSBUS 1 HIGH BATT | 11 | DSBUS 1 SELF TEST FAIL |
| | 4 | DSBUS 2 HIGH BATT | 12 | DSBUS 2 SELF TEST FAIL |
| | 5 | DSBUS 3 HIGH BATT | 13 | DSBUS 3 SELF TEST FAIL |
| | 6 | DSBUS 4 HIGH BATT | 14 | DSBUS 4 SELF TEST FAIL |
| | 7 | DSBUS 1 LOW BATT | 15 | PRIMARY AMP 1 FAIL |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|-----------------------------------|----|--|
| 460043 | 0 | PRIMARY AMP 2 FAIL | 8 | BACKUP AMP 1 NOT INSTALLED |
| | 1 | PRIMARY AMP 3 FAIL | 9 | BACKUP AMP 2 NOT INSTALLED |
| | 2 | PRIMARY AMP 4 FAIL | 10 | BACKUP AMP 3 NOT INSTALLED |
| | 3 | BACKUP AMP 1 FAIL | 11 | BACKUP AMP 4 NOT INSTALLED |
| | 4 | BACKUP AMP 2 FAIL | 12 | MODBUS COMMUNICATIONS FAULT |
| | 5 | BACKUP AMP 3 FAIL | 13 | VESDANET TROUBLE |
| | 6 | BACKUP AMP 4 FAIL | 14 | Reserved |
| | 7 | BACKUP AMP NOT INSTALLED | 15 | DOOR INTERLOCK FAULT |
| 460044 | 0 | ANNUN 01 TYPE MISMATCH | 8 | ANNUN 09 TYPE MISMATCH |
| | 1 | ANNUN 02 TYPE MISMATCH | 9 | ANNUN 10 TYPE MISMATCH |
| | 2 | ANNUN 03 TYPE MISMATCH | 10 | ANNUN 11 TYPE MISMATCH |
| | 3 | ANNUN 04 TYPE MISMATCH | 11 | ANNUN 12 TYPE MISMATCH |
| | 4 | ANNUN 05 TYPE MISMATCH | 12 | ANNUN 13 TYPE MISMATCH |
| | 5 | ANNUN 06 TYPE MISMATCH | 13 | ANNUN14 TYPE MISMATCH |
| | 6 | ANNUN 07 TYPE MISMATCH | 14 | ANNUN 15 TYPE MISMATCH |
| | 7 | ANNUN 08 TYPE MISMATCH | 15 | ANNUN 16 TYPE MISMATCH |
| 460045 | 0 | ANNUN 17 TYPE MISMATCH | 8 | ANNUN 25 TYPE MISMATCH |
| | 1 | ANNUN 18 TYPE MISMATCH | 9 | ANNUN 26 TYPE MISMATCH |
| | 2 | ANNUN 19 TYPE MISMATCH | 10 | ANNUN 27 TYPE MISMATCH |
| | 3 | ANNUN 20 TYPE MISMATCH | 11 | ANNUN 28 TYPE MISMATCH |
| | 4 | ANNUN 21 TYPE MISMATCH | 12 | ANNUN 29 TYPE MISMATCH |
| | 5 | ANNUN 22 TYPE MISMATCH | 13 | ANNUN 30 TYPE MISMATCH |
| | 6 | ANNUN 23 TYPE MISMATCH | 14 | ANNUN 31 TYPE MISMATCH |
| | 7 | ANNUN 24 TYPE MISMATCH | 15 | ANNUN 32 TYPE MISMATCH |
| 460046 | 0 | DISPLAY COMM LOSS | 8 | LOOP CARD 1 COMM LOSS |
| | 1 | ALARM DEVICES DISABLED | 9 | LOOP CARD 2 COMM LOSS |
| | 2 | SMOKE CONTROL DISABLED | 10 | LOOP CARD 3 COMM LOSS |
| | 3 | PANEL HAS REBOOTED | 11 | LOOP CARD 4 COMM LOSS |
| | 4 | ZONES DISABLED BY BRIGADE | 12 | LOOP CARD 5 COMM LOSS |
| | 5 | ALARM SIGNAL | 13 | LOOP CARD 6 COMM LOSS |
| | 6 | KERNEL CORRUPTED | 14 | LOOP CARD 7 COMM LOSS |
| | 7 | CHANGE SERVICE TOOL PASSWORD | 15 | LOOP CARD 8 COMM LOSS |
| 460047 | 0 | LOOP CARD 9 COMM LOSS | 8 | PMB 4 COMM LOSS |
| | 1 | LOOP CARD 10 COMM LOSS | 9 | PMB 5 COMM LOSS |
| | 2 | CHANGE MASTER USER PASSWORD | 10 | Recovery Partition Application Active |
| | 3 | PASSWORD DATABASE CORRUPTED | 11 | AIO COMM CLASS A TROUBLE |
| | 4 | Default database. Please program. | 12 | AC Failure (LSB is PMB address 1-5) |
| | 5 | PMB 1 COMM LOSS | 13 | Earth Fault (LSB is PMB address 1-5) |
| | 6 | PMB 2 COMM LOSS | 14 | Earth Fault Switch Mismatch (LSB is PMB address 1-5) |
| | 7 | PMB 3 COMM LOSS | 15 | Battery Low (LSB is PMB address 1-5) |

Table 7.33: System Troubles Register Map (Continued)

| | | | | |
|--------|---|--|----|---|
| 460048 | 0 | Battery High (LSB is PMB address 1-5) | 8 | AIO Address 5 Comm Loss (LSB is 0 for router, 1-15 for peripheral) |
| | 1 | Battery Deep-Discharge (LSB is PMB address 1-5) | 9 | AIO Address 6 Comm Loss (LSB is 0 for router, 1-15 for peripheral) |
| | 2 | Charger Fail (LSB is PMB address 1-5) | 10 | AIO Address 7 Comm Loss (LSB is 0 for router, 1-15 for peripheral) |
| | 3 | Power Supply Failure (LSB is PMB address 1-5) | 11 | AIO Address 8 Comm Loss (LSB is 0 for router, 1-15 for peripheral) |
| | 4 | AIO Address 1 Comm Loss (LSB is 0 for router, 1-15 for peripheral) | 12 | AIO Address 9 Comm Loss (LSB is 0 for router, 1-15 for peripheral) |
| | 5 | AIO Address 2 Comm Loss (LSB is 0 for router, 1-15 for peripheral) | 13 | AIO Address 10 Comm Loss (LSB is 0 for router, 1-15 for peripheral) |
| | 6 | AIO Address 3 Comm Loss (LSB is 0 for router, 1-15 for peripheral) | 14 | Reserved |
| | 7 | AIO Address 4 Comm Loss (LSB is 0 for router, 1-15 for peripheral) | 15 | Reserved |
| 460049 | 0 | POTS Card No Answer / Missing | 8 | Ethernet 1 No Connectivity |
| | 1 | POTS Line 1 Failure | 9 | Ethernet 2 No Connectivity |
| | 2 | POTS Line 2 Failure | 10 | CLSS Site Manager Communication Failure |
| | 3 | POTS Call (Alarm Routing) Failure | 11 | Ethernet/Wini Alarm Routing Failure |
| | 4 | POTS Software Mismatch | 12 | Cellular Alarm Routing Failure |
| | 5 | Cellular Card No Answer / Missing | 13 | Reserved |
| | 6 | Cellular Card No Connectivity | 14 | Reserved |
| | 7 | Wini No Connectivity | 15 | Reserved |

Section 8: The BACnet Feature

The BACnet feature of the CLSS Gateway provides communications between a network using the BACnet communication protocol and the gateway's FACP(s) in an NFN network or high-speed NFN network.

The CLSS Gateway acts like any other node on an NFN network or a high-speed NFN network. The NFN network communicates with the gateway through an HS-NCM-W/SF/MF or NCM-W/F network control module that is on that NFN network or through a direct connection to a single NOTIFIER® panel. The BACnet communication protocol is an *American National Standard (ANSI/ASHRAE 135-1995)*.

The CLSS BACnet client will present the physical fire devices in the network as BACnet objects. The CLSS Gateway manages their object database. As events occur, the object properties are updated in real-time, and messages are sent to the appropriate BACnet report destination.



NOTE: The BACnet computer clients are computers with a graphical user interface workstation front-end.

The BACnet clients may make requests to read properties of the BACnet objects. Those properties are the values of the device status and programming.

The user subscribes to Event Notification objects per FACP, and the BACnet device receives events from objects on the FACP as a result of this subscription. Large networks can use multiple gateways (greater than 15 panels/15,000 objects).

The BACnet client workstation front-end must conform to *BACnet Standard Annex J* for IP and support *Device Objects*, *Binary Output Objects*, and *Multi-state Input or Life Safety Points/Zones*. It is also required to write to Notification Objects and receive confirmed/unconfirmed event notification messages.

CLSS Gateway is configured through *CLSS App* and *CLSS Site Manager*. For information about configuration, refer to [“Configurations” on page 29](#).



NOTE: This manual is written with the understanding that its user is trained in BACnet operations and services. The information provided here is solely for the configuration of the Gateway to communicate event information to an existing BACnet network.

8.1 Agency Listings

**NOTE:**

UL 864, 9th Edition—This system works with products that have been UL 864, 9th Edition listed as well as products that have not received UL 864, 9th Edition certification. Operation of systems that are comprised of equipment that is UL 864, 9th Edition listed together with products that are not UL 864, 9th Edition listed requires the approval of the local Authority Having Jurisdiction (AHJ).

CAN/ULC-S559-04, 1st Edition—This system works with products that have been CAN/ULC-S559-04, 1st Edition listed as well as products that have not received CAN/ULC-S559-04, 1st Edition certification. Operation of systems that are comprised of equipment that is CAN/ULC-S559-04, 1st Edition listed together with products that are not CAN/ULC-S559-04, 1st Edition listed requires the approval of the local Authority Having Jurisdiction (AHJ).

8.1.1 Compliance

This product has been investigated to, and found to be in compliance with the following standards.

National Fire Protection Association

- NFPA 72—National Fire Alarm Code

Underwriters Laboratories

- UL-864—Control Units for Fire Alarm Systems, Ninth Edition
- UL-2017—General-Purpose Signaling Devices and Systems, First Edition

Underwriters Laboratories Canada

- CAN/ULC-S527-99—Standard for Control Units for Fire Alarm Systems, Second Edition
- CAN/ULC-S559-04—Equipment for Fire Signal Receiving Centres and Systems, First Edition

8.2 Installation

This product is intended to be installed in accordance with the following regulatory agencies.

Local

- AHJ—Authority Having Jurisdiction
- National Fire Protection Association
- NFPA 70—National Electrical Code
- NFPA 72—National Fire Alarm Code
- NFPA 101—Life Safety Code

Underwriters Laboratories

- UL-1076—In certified applications, the unit shall be installed in accordance with Proprietary Burglar Alarm Units and Systems, Fifth Edition

Underwriters Laboratories Canada

- CAN/ULC-S524-06—Standard for the Installation of Fire Alarm Systems, Fifth Edition
- CAN/ULC-S561-03—Installation and Services for Fire Signal Receiving Centres and Systems, First Edition

Canada

- CSA C22.1—Canadian Electrical Code, Part I, Safety Standard for Electrical Installations



WARNING: Improper installation, maintenance, and lack of routine testing could result in system malfunction.

8.3 Compatibility

Refer to “[CLSS Gateway Compatible Node Types](#)” on page 101 for supported panels and annunciators.

8.4 System Requirements

The CLSS Gateway can monitor up to fifteen panels, but the combined object count across the monitored panels cannot exceed 15,000 objects. This includes all detectors, monitor modules, control modules, bell circuits, and so on.

Refer to the NFN network manual for details about wiring limitations.

Access the configuration web page from a computer in the same IP subnet as the CLSS Gateway with latest version of Google Chrome. The latest version of JAVA must also be installed and enabled.

8.5 System Architecture



NOTE: The CLSS Gateway client workstation is not intended as a primary annunciator and is ancillary in nature.

These are connections options for the CLSS Gateway architecture.

An Internet or Intranet IP network connection is used with both architectures.

8.5.1 Single Panel Architecture

Direct panel connection — a connection is made directly to a supported NOTIFIER® panel or annunciator “[Single Panel Connecting to BACnet via CLSS Gateway](#)” on page 91. Refer to “[CLSS Gateway Compatible Node Types](#)” on page 101 for supported panels and annunciators.

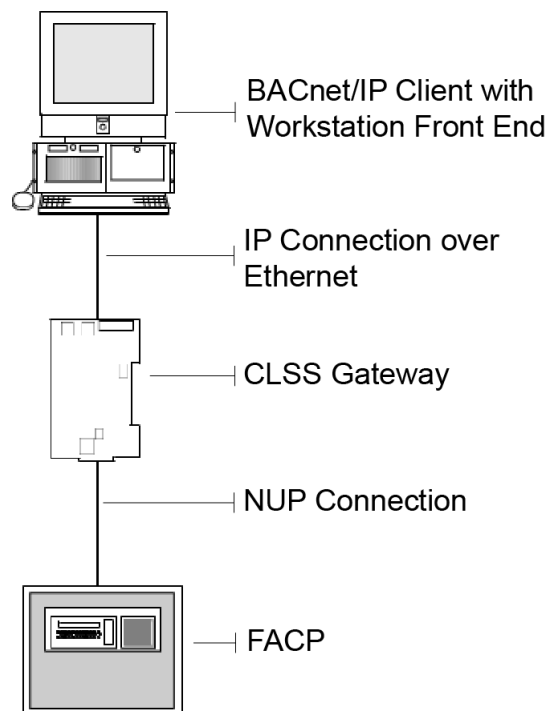


Figure 8.1: Single Panel Connecting to BACnet via CLSS Gateway

8.5.2 NFN Network Architecture

NFN network connection — a NUP connection is made to an NCM or HS-NCM board on the NFN network as the CLSS Gateway [Figure 8.2, “Notifier System Example 1- A Single NFN Network”](#).

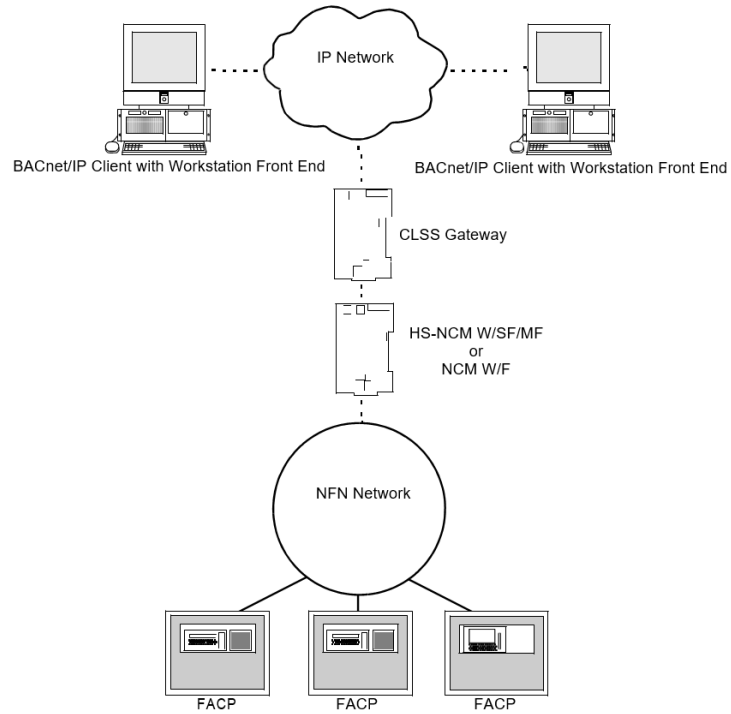


Figure 8.2: Notifier System Example 1- A Single NFN Network

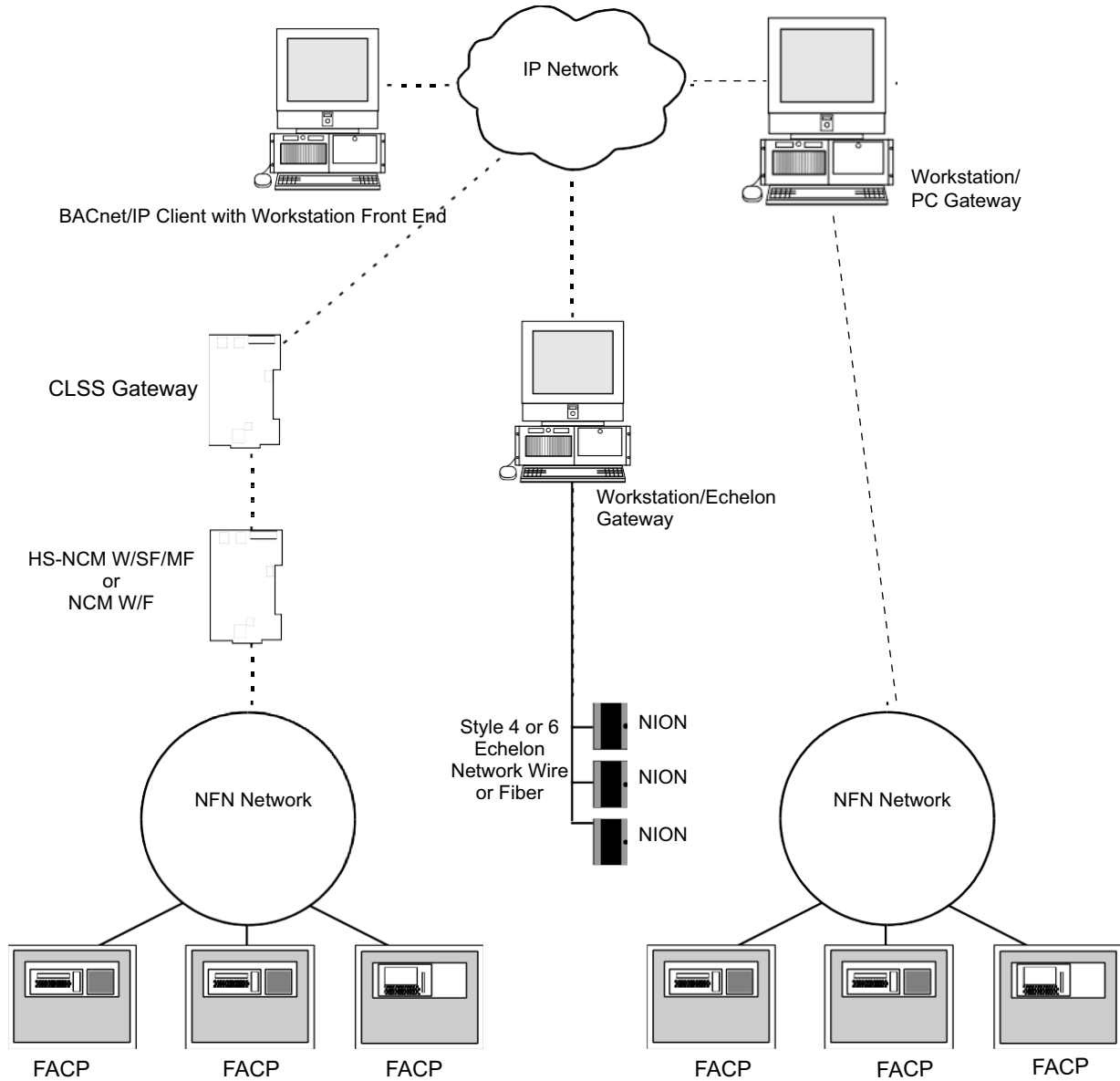


Figure 8.3: Notifier System Example 2 - Multiple NFN Networks

8.6 BACnet Feature Activation

Purchase the required number of BACnet support on *CLSS Site Manager* and then activate that feature in CLSS App.



NOTE: Purchase should be within the number of tokens available.

8.6.1 To Purchase the BACnet Support

1. Log onto *CLSS Site Manager*.
2. Click on your account name and select **Manage Access**.

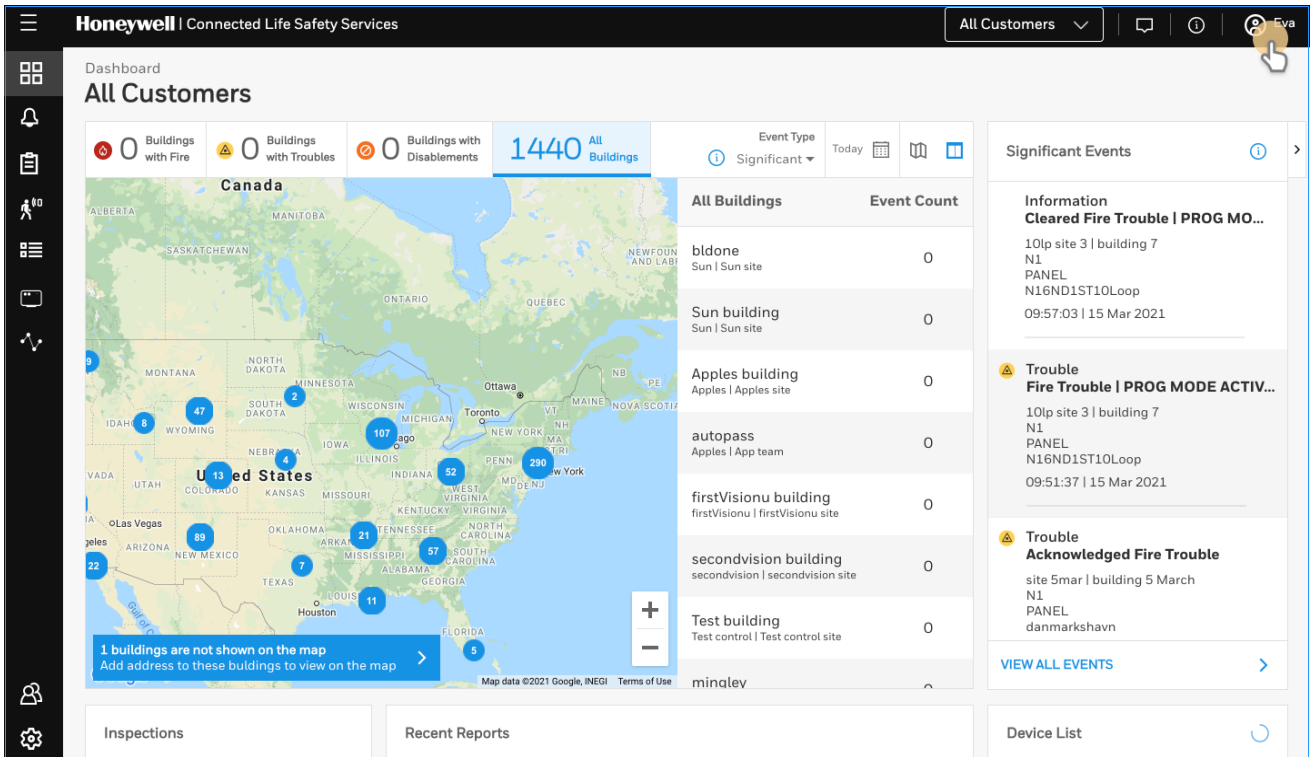


Figure 8.4: Selecting Manage Access

3. Click **Features** on the **Manage Access** page.
4. Click **Gateway** under the **Features** section.
5. Note down the purchased number under **Available Features**.
6. Click **PURCHASE** at the top right side.

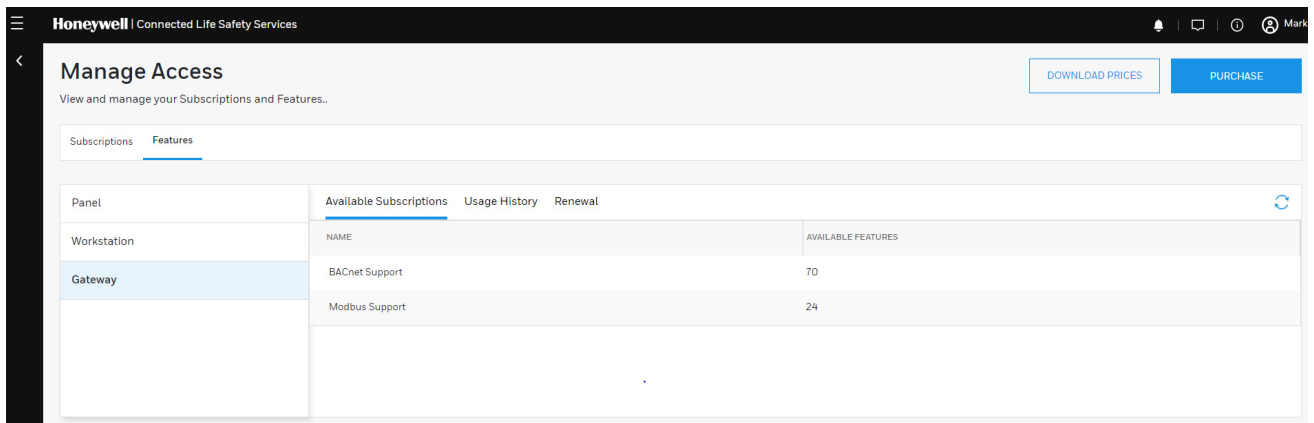


Figure 8.5: Purchasing the BACnet Support

7. Scroll down to find **BACnet Support** in the **Features** tab.
8. Enter the number of support required in the **BACnet Support** field.
9. Click **PURCHASE**.
10. Read the **Confirmation** message and if acceptable, click **CONFIRM**.
Or
Click **CANCEL** and repeat the steps from 8 to 10.
11. Wait for the purchase to complete and refresh the page, if required.
12. Verify that the purchased number under **Available Features** is correct.

8.6.2 To Activate the BACnet Support



NOTE:

- The gateway must be already installed. If not, install the fixed gateway.
- All the network settings should be configured while installing.

1. Tap **Perform Feature Activation** on the CLSS App's welcome message.

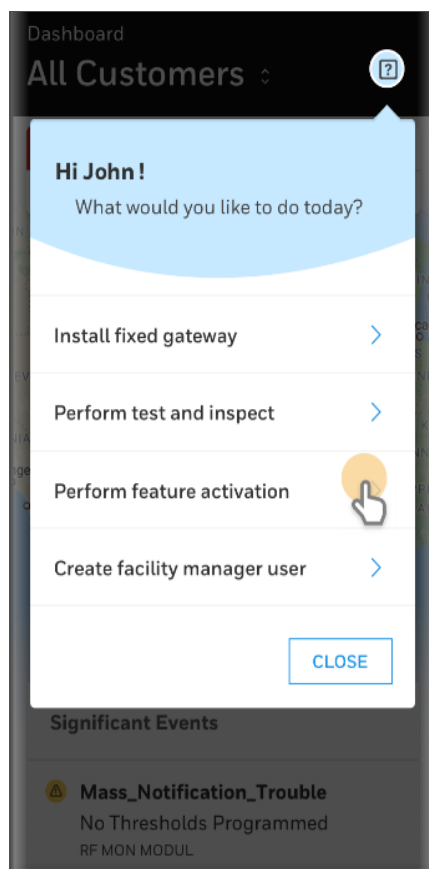


Figure 8.6: Feature Activation: The First Step

2. Tap **Fixed Gateways**.
3. Select the site of the gateway.
4. Find and tap the OC of the gateway.
5. Tap **ADD ACTIVATION**.
6. Tap **BACnet Support** under the **One Time Activations**.
7. Tap **ACTIVATE**.
8. Wait for the activation successful message.

8.6.3 Standard Object Types Supported—Life Safety Point/Life Safety Zone

| | | | |
|-----------------------|---------------------------|-------------------------------|---|
| Present Value | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | IssQuiet | Normal |
| | 1 | IssPreAlarm | PreAlarm |
| | 2 | IssAlarm | Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm, (Life/Property), Medical Emergency |
| | 3 | IssFault | Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device or Zone, Disabled, Non-Fire Device Disabled |
| | 7 | IssActive | Non-Fire Activation |
| | 22 | IssSupervisory | Supervisory (Equipment), Supervisory (Guard's Tour) |
| Tracking Value | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | IssQuiet | Normal |
| | 1 | IssPreAlarm | PreAlarm |
| | 2 | IssAlarm | Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm (Life/Property), Medical Emergency |
| | 3 | IssFault | Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device or Zone, Disabled, Non-Fire Device Disabled |
| | 7 | IssActive | Non-Fire Activation |
| | 22 | IssSupervisory | Supervisory (Equipment), Supervisory (Guard's Tour) |
| Event State | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | EsNormal | Normal |
| | 1 | EsFault | Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device Disabled, Non-Fire Device Disabled |
| | 2 | EsOffNormal | All statuses other than normal and fault. |
| Reliability | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | reNoFaultDetected | All statuses other than trouble. |
| | 7 | re_UnreliableOther | Security Trouble, Fire Trouble, Non-Fire Trouble |
| Mode | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | IsmOff | Power-Up State |
| | 11 | IsmEnabled | Set if point has been disabled and subsequently enabled since startup. |
| | 12 | IsmDisabled | Fire Device or Zone Disabled, Non-Fire Device Disabled |

| | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
|-----------------------------|-----------------------------|-------------------------------|---|
| Silence State | 0 | ssUnsilenced | Audibles Unsilenced |
| | 1 | ssAudiblesSilenced | Audibles Silenced |
| Operation Expected | BACnet Enumeration | | NFN State |
| | 0 | | NA |
| Maintenance Expected | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | NA | NA | NA |
| Event Enable | BACnet Event Transition Bit | | |
| | | toOffNormal | |
| | | toFault | |
| Direct Reading | REAL | NA | % Alarm |
| Status Flags | Boolean | BACnet Status Flags | NFN State |
| | 0,0,0,0 | | Normal |
| | 1,0,0,0 | InAlarm | Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm (Life/Property), Medical Emergency |
| | 1,1,0,0 | InAlarm, Fault | Security Trouble, Fire Trouble, Non-Fire Trouble, PreAlarm |
| | 1,0,0,1 | InAlarm, OutOfService | Fire Device or Zone Disabled, Non-Fire Device Disabled |
| Out of Service | Boolean | | NFN State |
| | 0 | FALSE | All statuses other than disable |
| | 1 | TRUE | Fire Device or Zone Disabled, Non-Fire Device Disabled |

8.6.4 Standard Object Types Supported—Multi-State Input Standard Object Types

| | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
|----------------------|---------------------------|-------------------------------|--|
| Present Value | 1 | None | Normal |
| | 2 | None | All statuses other than those included in 3 and 4 below. |
| | 3 | None | Security Trouble, Fire Trouble, Non-Fire Trouble |
| | 4 | None | Fire Device or Zone Disabled, Non-Fire Device Disabled |

| Event State | BACnet Enumeration | BACnet Event State | NFN State |
|-----------------------|---------------------------|-------------------------------|---|
| | 0 | EsNormal | Normal |
| | 1 | EsFault | Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device Disabled, Non-Fire |
| | 2 | EsOffNormal | All statuses other than normal and fault. |
| Reliability | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | reNoFaultDetec | All statuses other than trouble. |
| | 7 | re_UnreliableOt | Security Trouble, Fire Trouble, Non-Fire |
| Status Flags | Boolean | BACnet Status Flags | NFN State |
| | 0,0,0,0 | | Normal |
| | 1,0,0,0 | InAlarm | Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm (Life/Property), |
| | 1,1,0,0 | InAlarm, Fault | Security Trouble, Fire Trouble, Non-Fire Trouble, PreAlarm |
| | 1,0,0,1 | InAlarm, OutOfService | Fire Device or Zone Disabled, Non-Fire Device Disabled |
| Out of Service | Boolean | | NFN State |
| | 0 | FALSE | All statuses other than disable |
| | 1 | TRUE | Fire Device or Zone Disabled, Non-Fire |

8.6.5 Supported—Binary Output

| | | | |
|-----------------------|---------------------------|-------------------------------|---|
| Present Value | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | IssQuiet | Normal |
| | 1 | IssPreAlarm | PreAlarm |
| | 2 | IssAlarm | Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm, (Life/Property), Medical Emergency |
| | 3 | IssFault | Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device or Zone, Disabled, Non-Fire Device Disabled |
| | 7 | IssActive | Non-Fire Activation |
| | 22 | IssSupervisory | Supervisory (Equipment), Supervisory (Guard's Tour) |
| Tracking Value | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | IssQuiet | Normal |
| | 1 | IssPreAlarm | PreAlarm |
| | 2 | IssAlarm | Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm (Life/Property), Medical Emergency |
| | 3 | IssFault | Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device or Zone, Disabled, Non-Fire Device Disabled |
| | 7 | IssActive | Non-Fire Activation |
| | 22 | IssSupervisory | Supervisory (Equipment), Supervisory (Guard's Tour) |
| Event State | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | EsNormal | Normal |
| | 1 | EsFault | Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device Disabled, Non-Fire Device Disabled |
| | 2 | EsOffNormal | All statuses other than normal and fault. |
| Reliability | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | reNoFaultDetected | All statuses other than trouble. |
| | 7 | re_UnreliableOther | Security Trouble, Fire Trouble, Non-Fire Trouble |

| Mode | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
|----------------------|-----------------------|--|---|
| | 0 | IsmOff | Power-Up State |
| 11 | IsmEnabled | Set if point has been disabled and subsequently enabled since startup. | |
| 12 | IsmDisabled | Fire Device or Zone Disabled, Non-Fire Device Disabled | |
| Silence State | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | ssUnsilenced | Audibles Unsilenced |
| 1 | ssAudiblesSilenced | Audibles Silenced | |
| Operation Expected | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | 0 | | NA |
| Maintenance Expected | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | NA | NA | NA |
| Event Enable | BACnet Enumeration | BACnet LifeSafetyState | NFN State |
| | | toOffNormal | |
| | | toFault | |
| Direct Reading | REAL | NA | % Alarm |
| Status Flags | Boolean | BACnet Status Flags | NFN State |
| | 0,0,0,0 | | Normal |
| | 1,0,0,0 | InAlarm | Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm (Life/Property), Medical Emergency |
| | 1,1,0,0 | InAlarm, Fault | Security Trouble, Fire Trouble, Non-Fire Trouble, PreAlarm |
| 1,0,0,1 | InAlarm, OutOfService | Fire Device or Zone Disabled, Non-Fire Device Disabled | |
| Out of Service | Boolean | | NFN State |
| | 0 | FALSE | All statuses other than disable |
| | 1 | TRUE | Fire Device or Zone Disabled, Non-Fire Device Disabled |

8.6.6 Standard Object Types Supported—Notification Class

Write Property/Add List element required for Intrinsic Reporting.

Data Link Layer Options:

- BACnet IP, (Annex J)
- BACnet IP, (Annex J), Foreign Device
- ISO 8802-3, Ethernet (Clause 7)
- ANSI/ATA 878.1, 2.5 Mb. ARCNET (Clause 8)
- ANSI/ATA 878.1, RS-485 ARCNET (Clause 8), baud rate(s):
- MS/TP MASTER (Clause 9), baud rate(s):
- MS/TP SLAVE (Clause 9), baud rate(s):
- Point-To-Point, EIA 232 (Clause 10), baud rate(s):
- Point-To-Point, modem, (Clause 10), baud rate(s):
- LonTalk, (Clause 11), medium:
- Other:

Device Address Binding:

Is static device binding supported? (This is currently necessary for two-way communication with MS/TP slaves and certain other devices.)

- Yes
- No

Networking Options:

- Router, Clause 6—List all routing configurations, e.g., ARCNET-Ethernet, Ethernet-MS/TP, etc. BACnet to Proprietary ARCnet Fire Network
- Annex H, BACnet Tunneling Router over IP BACnet Broadcast Management Device (BBMD)

Does the BBMD support registrations by Foreign Devices?

- Yes
- No

Character Sets Supported:

Indicating support for multiple character sets does not imply that they can all be supported simultaneously.

- ANSI X3.4
- IBM/Microsoft DBCS ISO 8859-1
- ISO 10646 (UCS-2)
- ISO 10646 (ICS-4)
- JIS C 6226

8.6.7 Supported Non-BACnet Equipment/Networks

This product supports communications between NOTIFIER® Fire and Annunciator nodes compatible with network v5.0 and later operating in a network or stand-alone configuration.

8.7 CLSS Gateway Compatible Node Types



NOTE: The CLSS Gateway requires that at least one node on the NFN network be an ONYX series panel. The gateway does not operate on an NFN network with no ONYX series panels.

8.7.1 Direct Connect Node Type Compatibility

Refer to [“Connecting to the Panels”](#) on page 105.

Table 8.1: Table B.1 Panel Communication Connection Table

| Supported Panel Types |
|-----------------------|
| AFP-2800 |
| AFP-3030 |
| N16 (INSPIRE) |
| NCM |
| NFS-3030 |
| NFS-3030 |
| NFS-320 |
| NFS-320 |
| NFS-640 |
| NFS-640 |
| NFS2-3030 |
| NFS2-3030 |
| NFS2-640 |
| NFS2-640 |
| XLS-120 |
| XLS-140-2 |
| XLS-2000 |
| XLS-3000 |

Appendix A: Gateway Operating Conditions

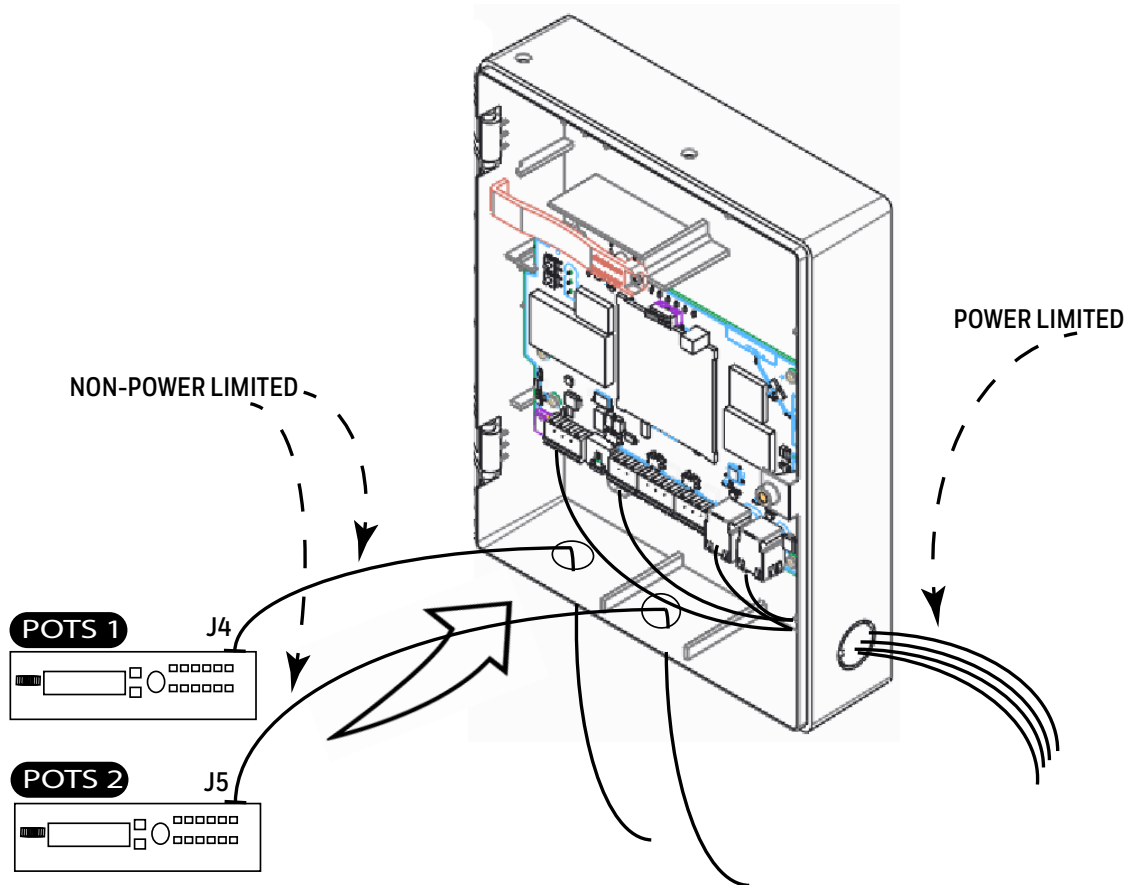
Table A.1: Operational Requirements

| Power Requirements | |
|-------------------------|--|
| Working voltage range | 18V - 30V DC |
| Current | For HON-CGW-DACT: 180mA (maximum) For HON-CGW-MBB: 140mA (maximum) NOTE: The power requirement varies with the number of interfaces used. |
| Location Requirements | |
| Room Temperature | 15 - 27° C (60 - 80° F) |
| Operational Temperature | 0° C - 49° C (32° F - 120° F) |
| Relative humidity | 93% ± 2% RH (Non-condensing) at 32° C ± 2° C (90° F ± 3° F) |



CAUTION: THE USEFUL LIFE OF THE SYSTEM'S STANDBY BATTERIES AND THE ELECTRONIC COMPONENTS MAYBE ADVERSELY AFFECTED BY EXTREME TEMPERATURE RANGES AND HUMIDITY. THEREFORE, IT IS RECOMMENDED THAT THIS SYSTEM AND ITS PERIPHERALS BE INSTALLED IN AN ENVIRONMENT WITH A NORMAL ROOM TEMPERATURE OF 15 - 27° C (60 - 80° F).

A.1 Wirings and Power



Appendix B: Modulations and Power Used

Radio devices operating on the below frequencies should not be installed next to each other.

Target Power that Meets Spectrum Mask and EVM Compliance

Table B.1: Wireless Power Specifications

| 2.4 GHz TX Power Specifications | | | | | | | |
|---------------------------------|-----------|--------------|--------|---------------------------|------------|-------|-----------|
| IEEE 802.11 | Mod | Rate | BW | Channel | Spec (TYP) | Units | Tol. (dB) |
| 11b | CCK, DSSS | 1 to 11 Mbps | 20 MHz | 1-13 | 17.5 | dBm | +/-2.0 |
| 11g | OFDM | 6 to 54 Mbps | 20 MHz | 1-13 | 15 | dBm | +/-2.0 |
| 11n | OFDM | MCS 0-7 | 20 MHz | 1-13 | 15 | dBm | +/-2.0 |
| 5 GHz TX Power Specifications | | | | | | | |
| Std | Mod | Rate | BW | Channel | Spec (TYP) | Units | Tol. (dB) |
| 11a | OFDM | 6-54 Mbps | 20 MHz | 36-48 52-64 100-144 | 15 | dBm | +/-2.0 |
| 11n | OFDM | MCS 0-7 | 20 MHz | 36-48 52-64 100-144 | 15 | dBm | +/-2.0 |

Appendix C: Connecting to the Panels

C.1 Gateway Board Connections

The gateway board can connect with a cellular module, wireless aerials, the *CLSS Site Manager*, a configuration computer, a panel, a mobile device, and an external power supply.

Figure C.1 illustrates the connection options at the top side of the gateway board.

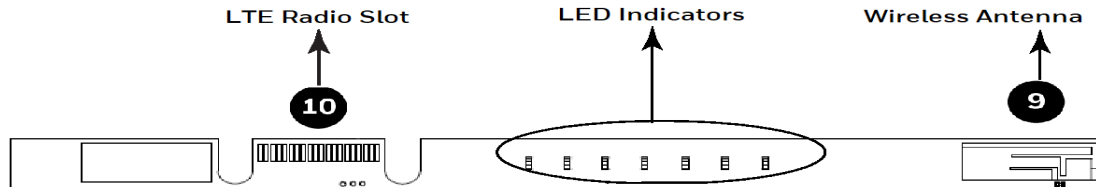


Figure C.1: Gateway Connections - Top Side

Figure C.2 illustrates the gateway connection options at the bottom side of the gateway board.

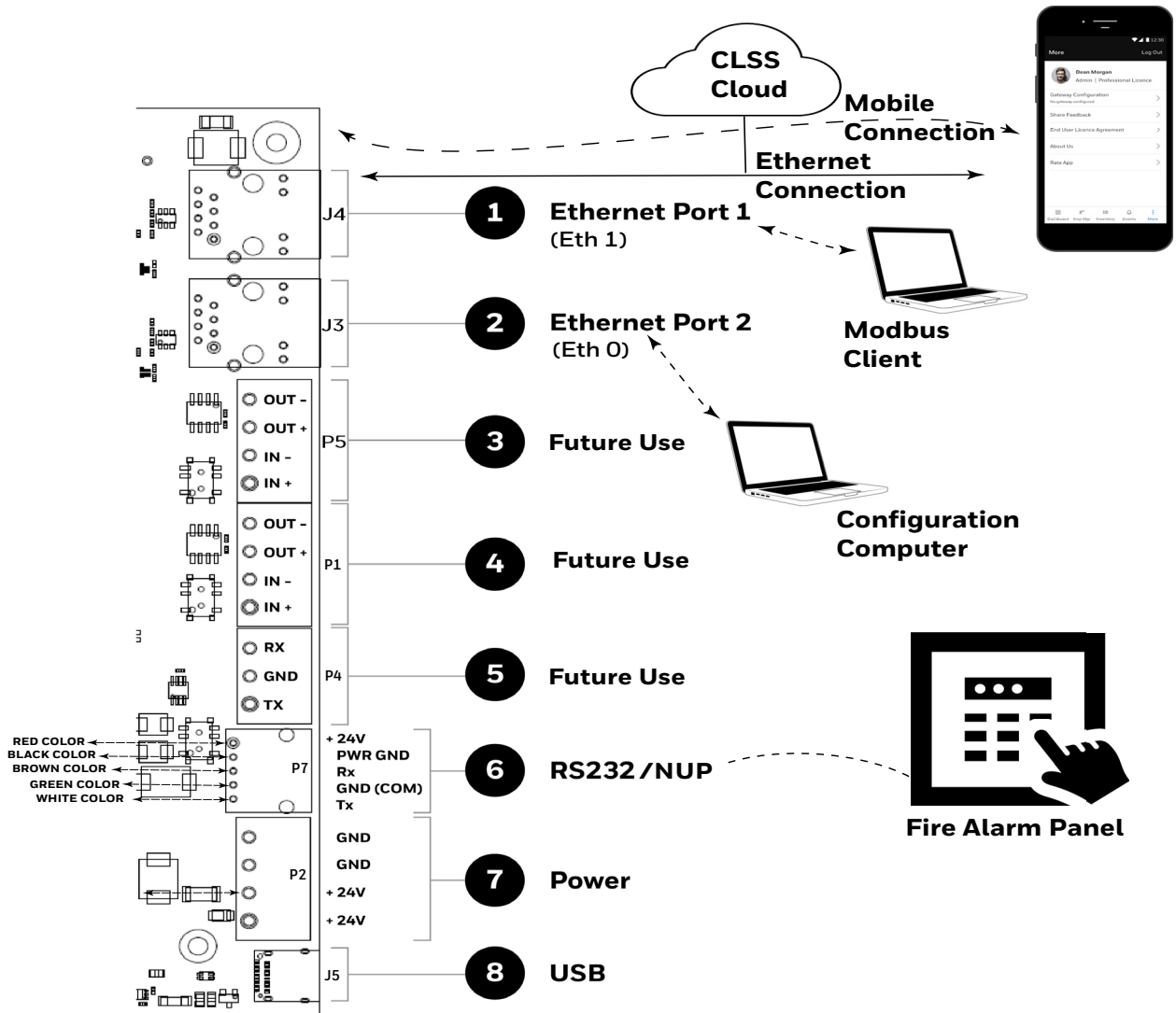


Figure C.2: Gateway Connection Options - Bottom Side

C.1.1 Connecting to a Fire Alarm Panel

The panel sends data from all its devices to the connected CLSS Gateway. The data transmission is based on the connection type and the panel compatibility.



WARNING: WHILE THE GATEWAY IS WORKING DO NOT REMOVE CONNECTIONS TO THE GATEWAY, CLSS SITE MANAGER, AND THE PANEL.



NOTE: When the gateway is communicating to a central station through cellular connection, it uses the primary Ethernet connection for *CLSS Site Manager* communications.



NOTE: The interfaces of the gateway board and the panels must be connected only with compatible cables, devices, and wirings.



NOTE: The total power a panel can distribute among its connected devices is limited. Therefore, before connecting the CLSS Gateway to a panel, ensure that the panel can continue to supply the required power to the gateway as well as other connected peripherals.
Refer to the panel and other peripherals' documents to know their power requirements.

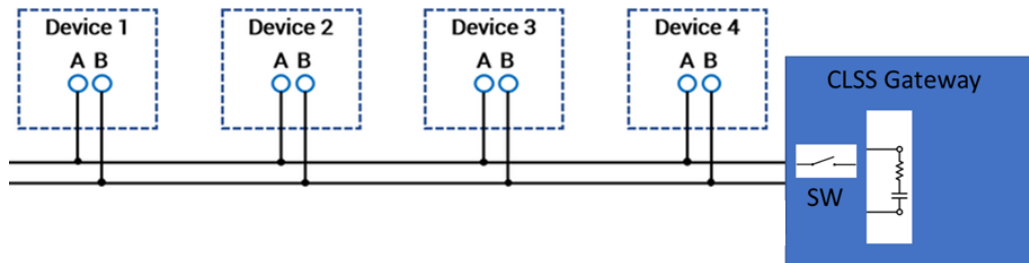
Improving the Signal Fidelity

An RS-485 loop of a panel with long cable and multiple devices may affect the signal fidelity. The gateway at the end of such an RS-485 loop can improve the signal fidelity with its termination resistor.

To enable the termination resistor on the gateway board:

If RS-485A is connected, switch the S4 switch to ON. If RS-485B is connected, switch the S5 switch to ON.

When there are no signal issues or when the gateway is not at the end of the loop, ensure that the S4 and S5 switches are switched to OFF.



C.2 Supported Panels

The CLSS Gateway supports the following panel variants:

- [AM Series Panels](#)
- [ESSER Panels](#)
- [Farenhyt Panels](#)
- [FireWarden Panels](#)
- [Gamewell-FCI Panels](#)
- [Gent Panels](#)
- [Morley-IAS Panels](#)
- [NOTIFIER® UL](#)
- [NOTIFIER® European Panels \(EN\)](#)
- [Silent Knight Panels](#)
- [Triga Panels](#)
- [VESDA® Detectors](#)

C.3 AM Series Panels

C.3.1 Connection Options

The gateway operates only with the AM Series fire alarm control panels listed in the table below:

Table C.1: AM Series Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | RS-232 | USB |
|-------------------------|--------|----------|------------------|-----|
| AM8200 | No | No | Yes ¹ | No |

¹ Use the SIB 8200 board



NOTE: The panel can be a stand alone panel or part of a network of panels.

Minimum Required Versions

For the Panel/CPU1: v1.0.703 | For SIB version Panel: v0.68

For the CLSS Gateway: 3.0.4.56

C.3.2 To Use an RS-232 Connection

Using an RS-232 cable the CLSS Gateway and the panel are connected.

The RS-232 port in the gateway board is labeled as 6 in the [Figure C.2](#).

1. On the Gateway Side

Connect to an RS-232 port of the gateway board.

2. On the Panel Side

- [AM8200 Panels](#)
- **AM8200 Panels**
 - Connect the White wire to the RX pin of the SIB 8200 board.
 - Connect the Green wire to the GND pin of the SIB 8200 board.
 - Connect the Brown wire to the TX pin of the SIB 8200 board.



NOTE: Because the SIB 8200 board on the panel connects to the gateway, the SIB board cannot be used for printing the events.

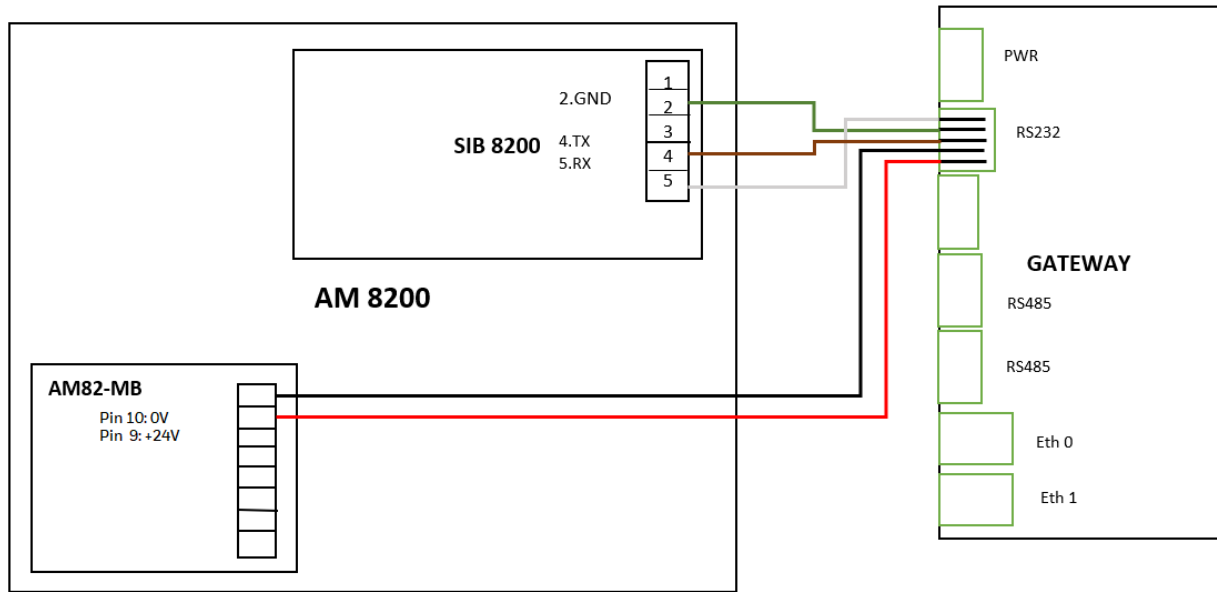


Figure C.3: Wiring Diagram: RS-232 Connection with AM8200 Panel

Power Connection

Using a power cable, the gateway can connect to the 24V DC power supply module of the AM8200 panel.



NOTE:

- Use the details given on the power supply module of the panel.
- The panel's power supply to the gateway must be within +24V DC power.

On the Gateway Side

- Ensure that the RS-232 cable is connected in the RS-232 port of the gateway.

On the Panel Side

- Connect the Red wire to the +ve pin of the AM82-MB board.
- Connect the Black wire to the -ve pin of the AM82-MB board.

C.4 ESSER Panels

The gateway should have an RS-485 connection with the panel for sending events. If *Inventory Synchronization* is required, use the RS-232 connection.

C.4.1 Connection Options

The gateway operates only with the ESSER fire alarm control panels as listed in the table below:

Table C.2: ESSER Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | RS-232 | USB |
|-------------------------|------------------------|----------|------------------|-----|
| FlexES Control | Yes | No | Yes ¹ | No |
| IQ8Control C | Yes ^{2 and 3} | No | Yes ¹ | No |
| IQ8Control M | Yes ^{2 and 3} | No | Yes ¹ | No |

1 Use a TTY-RS-232 converter (764856)

2 Use the RS-485 module (784871)

3 Use the add-on SEI-2 (Serial Essernet® Interface) (784850)

Minimum Required Versions

FlexES panel: 4.07R001

IQ8 panel: 03.13R000

CLSS Gateway: 3.1.4.72

C.4.2 To Use an RS-485 Connection

Using an RS-485 cable the CLSS Gateway and the panel are connected.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the [Figure C.2](#).

1. On the Gateway Side

Connect to an RS-485 port of the gateway board.

2. On the Panel Side

- [FlexES Panels](#)
- [IQ8 Panels](#)
- **FlexES Panels**
 - Connect the +ve wire to the Terminal 1 of the panel.
 - Connect the -ve wire to the Terminal 2 of the panel.

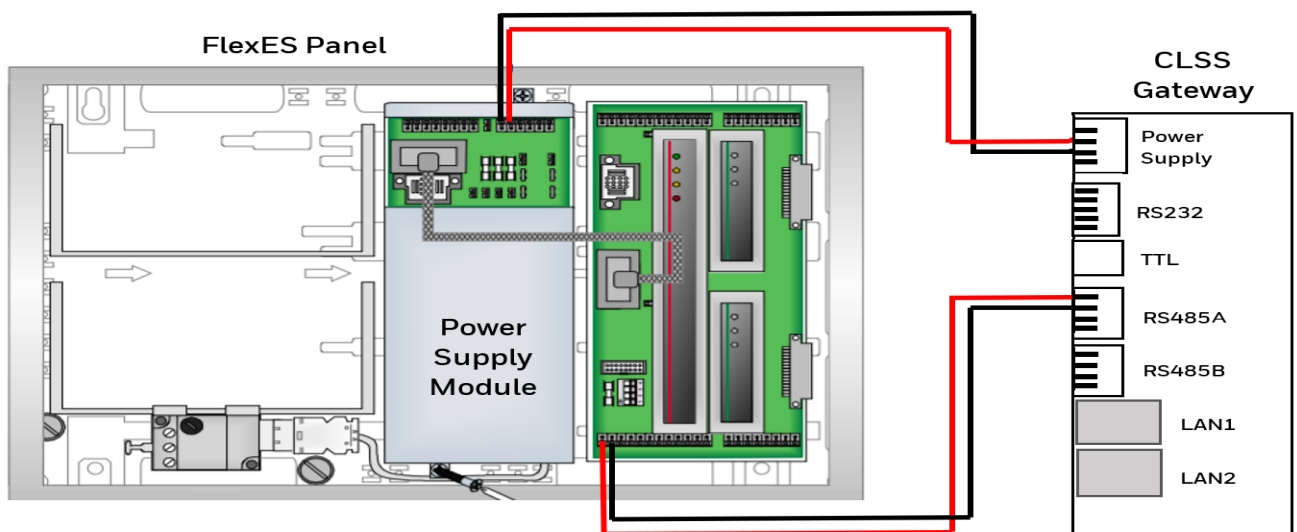


Figure C.4: Wiring Diagram: RS-485 Connections for a FlexES Panel

C.4.3 To Use an RS-232 Connection

Using an RS-232 cable, you can connect to the TTY port of the panel's serial interface.

1. On the Gateway Side

Connect the RS-232 cable with pre-formed connector to the RS-232 port of the gateway board.

Tip: The RS-232 port in the gateway board is labeled as 6 in the [Figure C.2](#).

2. On the TTY-RS-232 Converter Side

From the gateway:

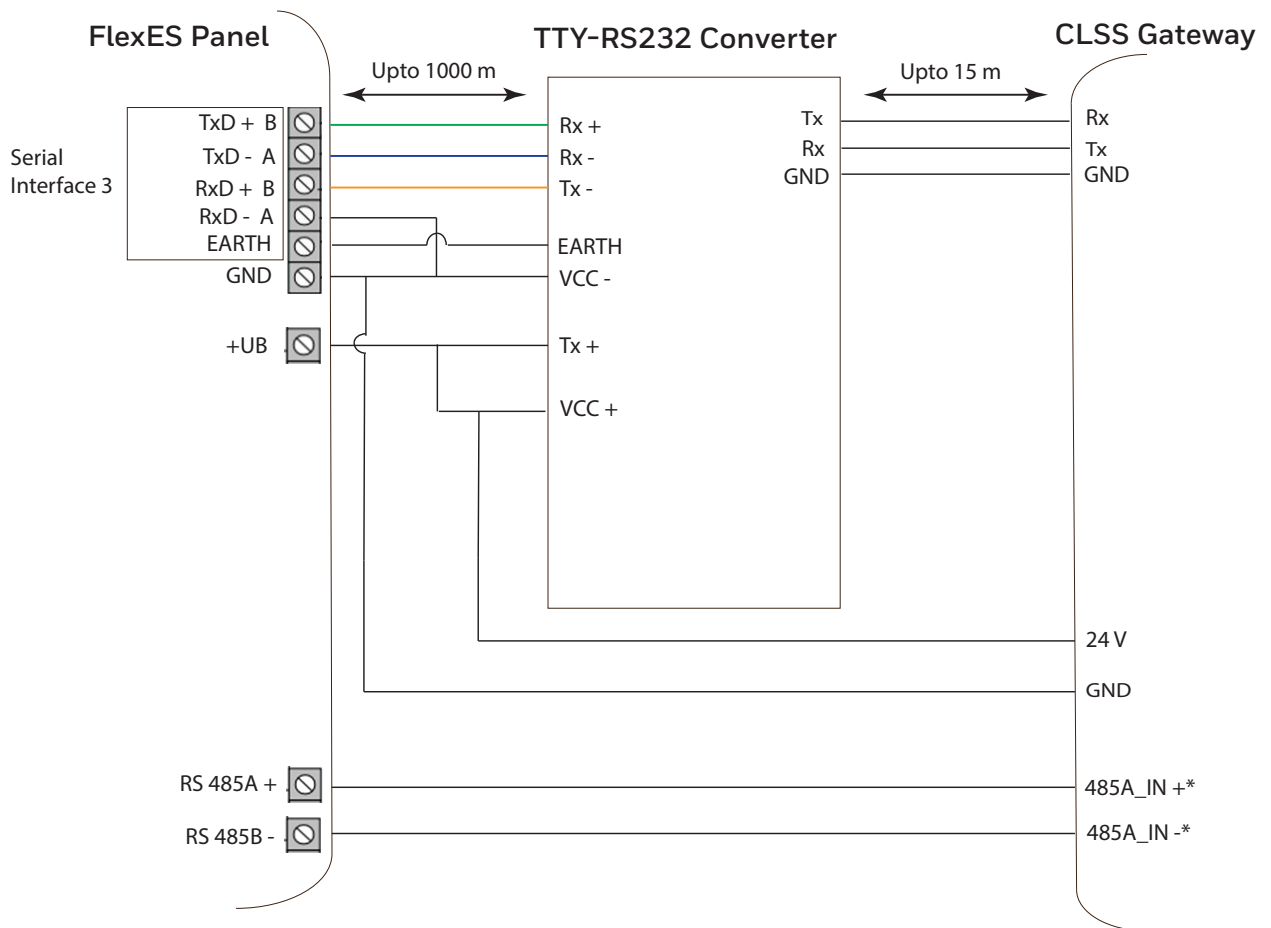
- Connect the Rx wire to the Tx pin of the TTY-RS-232 converter.
- Connect the Tx wire to the Rx pin of the TTY-RS-232 converter.

3. On the Panel Side

- [FlexES Panels](#)

• **FlexES Panels**

Connect as below:



*The connection can also be to 485B_IN + and 485B_IN -.

Figure C.5: Complete Setup with Both RS-485 and RS-232 Connections

4. Power Connection

Using a power cable, the gateway can connect to the 24V DC power supply module of the FlexES panel.



NOTE: Use the details given on the power supply module of the panel.



NOTE: The panel's power supply to the gateway must be within +24V DC power.

On the Gateway Side

- Connect the +ve wire to the +ve pin of the power supply port.
- Connect the -ve wire to the -ve pin of the power supply port.

On the Panel Side

- Connect the +ve wire to the +Ub pin of the power supply module.
- Connect the -ve wire to the Gnd pin of the power supply module.

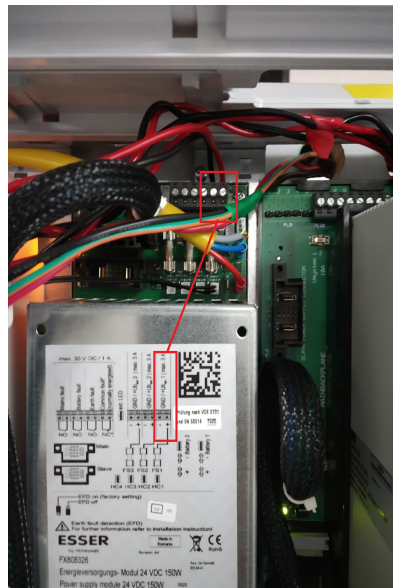


Figure C.6: FlexES Panel Power Connectors

C.4.4 Tools 8000 Settings

1. Select the **Serial Interfaces** tab in Tools 8000.
2. Go to the **Serial Interface 1** section.
3. Select *WINMANG* from the **Device in use** list.
4. Go to the **Serial Interface 3** section.
5. Select *Remote Access* from the **Device in use** list.
6. Click **OK**.

The screenshot shows the 'Controller Module' window with the 'Serial Interfaces' tab selected. The window is divided into three sections for Serial Interface 1, 2, and 3. Each section has a 'Type of interface' dropdown, a 'Device in use' dropdown, and a 'Label text' input field. The 'OK' button is highlighted with a blue border.

| Serial Interface | Type of interface | Device in use | Label text | Terminal Assignment |
|--------------------|-------------------|---------------|--------------|----------------------------------|
| Serial Interface 1 | RS 485 | WINMANG | CLSS-GW | Primary Loop 112 / Terminals 1+2 |
| Serial Interface 2 | RS 485 | WINMANG | FIRE BRIGADE | Primary Loop 112 / Terminals 3+4 |
| Serial Interface 3 | TTY | Remote access | CLSS-GW | intern |

• **IQ8 Panels**

To Use an RS-485 Connection

Using an RS-485 cable, you can connect to the additional RS-485 module (784871) on the panel's serial interface port.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the [Figure C.2](#).

On the Panel Side

Using an SEI2 Card Connect to the RS-485 (784871) module in the panel as below:

In the RXD port of the panel's SEI-2 card:

- Connect the In+ wire to the RXD+ pin.
- Connect the In- wire to the RXD- pin.

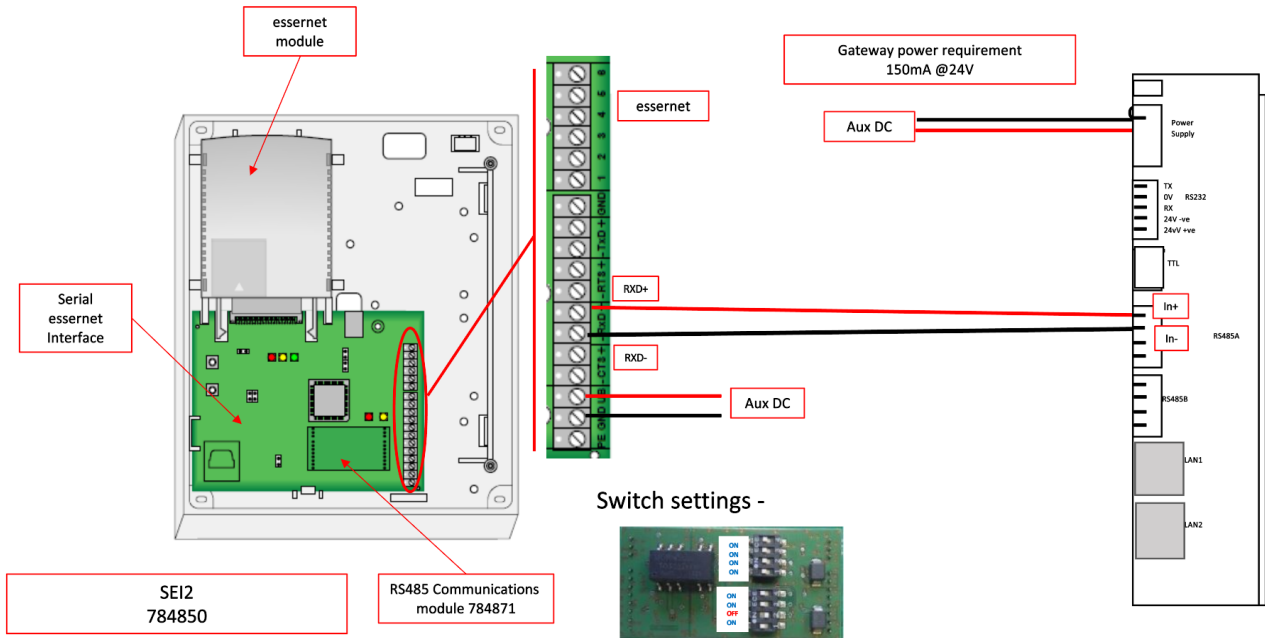


Figure C.7: Wiring Diagram: RS-485 to SEI2 Connection

Power Connection

Using a power cable, the gateway can connect to the 12V DC power supply module of the panel.



NOTE: Although the gateway is capable of receiving 24V DC power, it can work with the 12V DC power of the IQ8 panel. Ensure that the power supply to the gateway is within +12V DC power.

On the Gateway Side

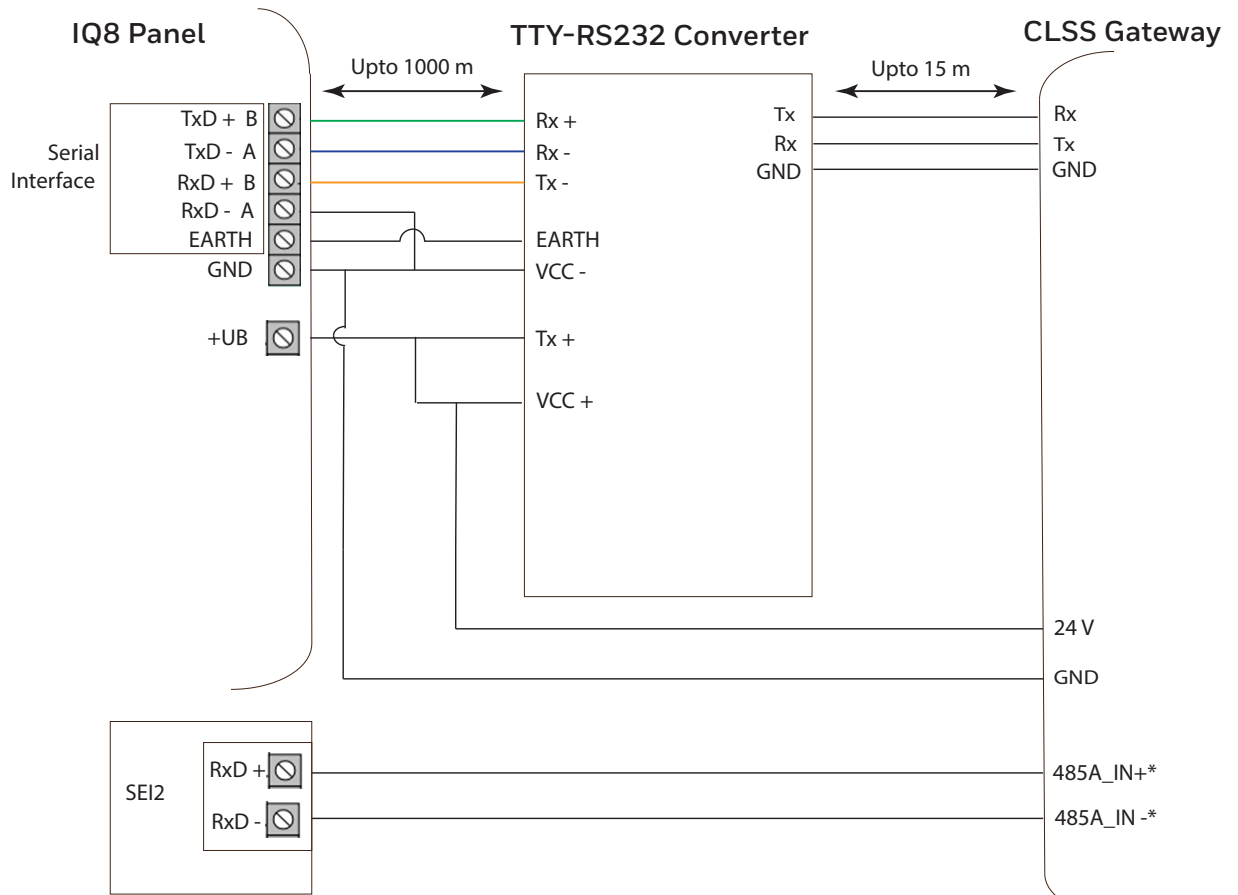
- Connect the +ve wire to the +ve pin of the power supply port.
- Connect the -ve wire to the -ve pin of the power supply port.

On the Panel Side

- Connect the +ve wire to the +UBext pin of the SEI-2 card.
- Connect the -ve wire to the GND pin of the SEI-2 card.

• **Connecting to Panel's TTY Port**

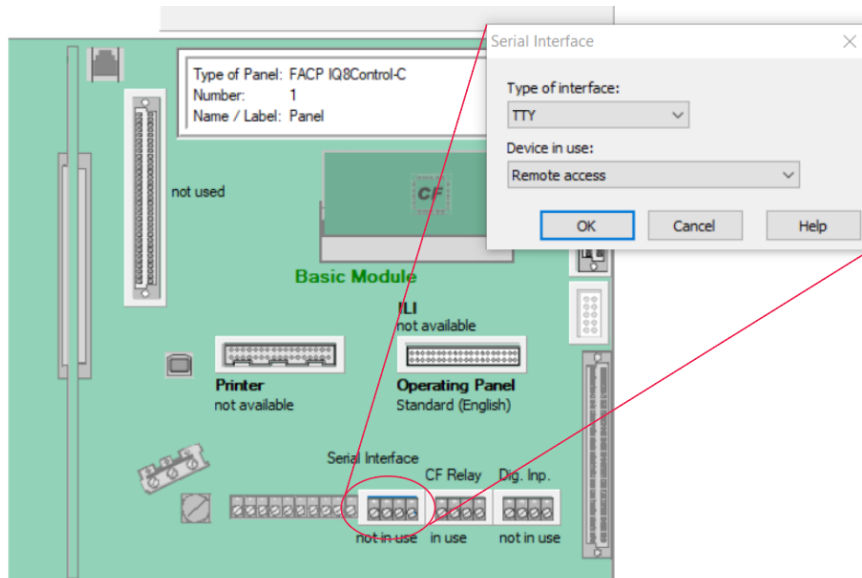
Using an RS-232 cable, you can connect to the RS-232 port on the panel's serial interface.



* The connection can also be to 485B_IN + and 485B_IN -.

C.4.5 Tools 8000 Settings

1. Double click on **Serial Interface** in Tools 8000.
2. Select **RS-232** from the **Type of interface** list.
3. Select **Remote Access** from the **Device in use** list.
4. Click **OK**.



5. Power Connection

Using a power cable, the gateway can connect to the 12V power supply module of the IQ8 panel.



NOTE: Use the details given on the power supply module of the panel.



NOTE: Although the gateway is capable of receiving 24V DC power, it can work with the 12V DC power of the IQ8 panel. Ensure that the power supply to the gateway is within +12V DC power.

On the Gateway Side

- Ensure that the RS-232 cable is connected in the RS-232 port of the gateway.
- Switch the S7 Switch next to the RS-232 port towards *NUP_IN*.

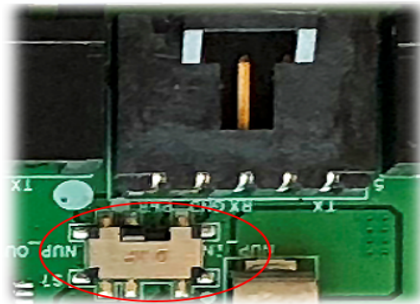


Figure C.8: The S7 Switch

On the Panel Side

- Connect the +ve wire to the +Ub pin of the SEI card.
- Connect the -ve wire to the Gnd pin of the SEI card.

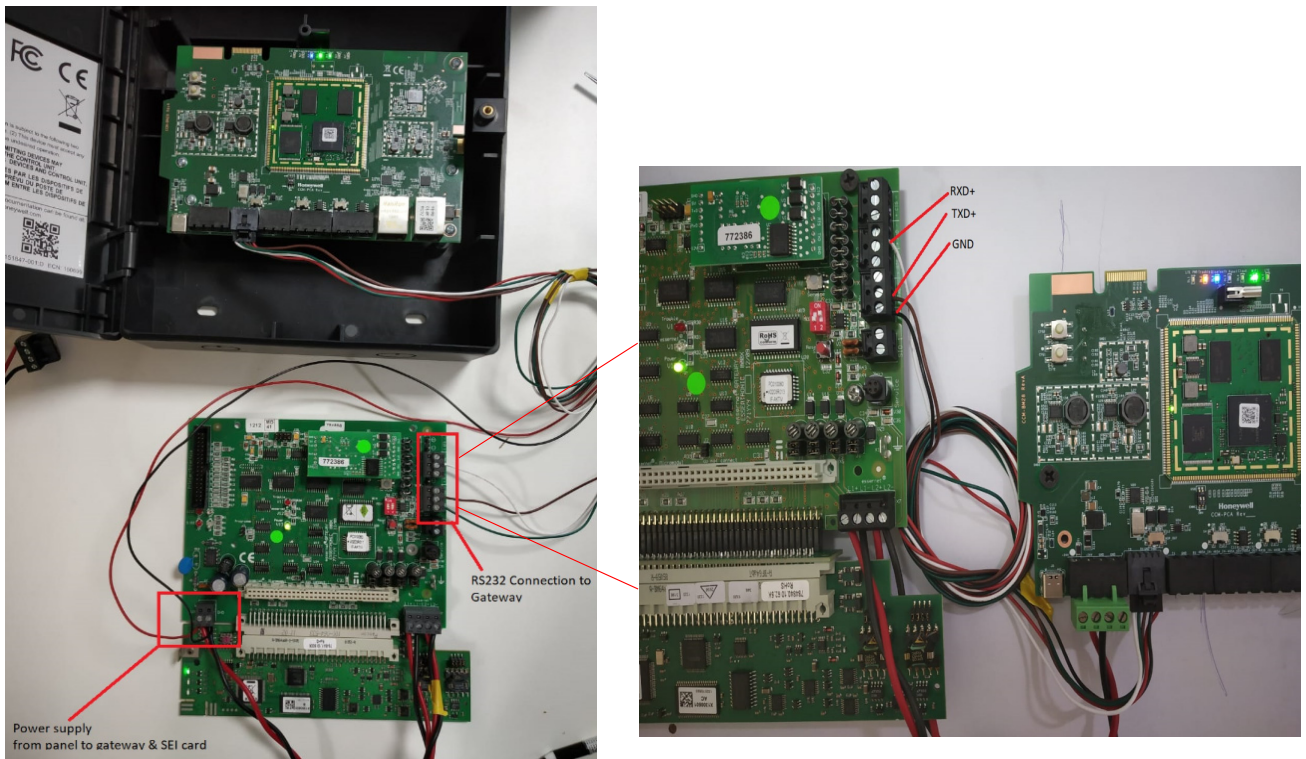


Figure C.9: IQ8 Panel RS-232 Power Connectors

C.5 Farenhyt Panels

C.5.1 Connection Options

The gateway operates only with the Farenhyt fire alarm control panels as listed in the table below:

Table C.3: Farenhyt Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | RS-232 | USB |
|--|--------|----------|--------|-----|
| Panel firmware version: 6.05.01 | | | | |
| IFP-75 | Yes | No | No | No |
| IFP-300 | Yes | No | No | No |
| IFP-300ECS | Yes | No | No | No |
| IFP-2100 | Yes | No | No | No |
| IFP-2100ECS | Yes | No | No | No |
| Panel firmware version: 5.0 | | | | |
| IFP-50 | Yes | No | No | No |
| IFP-100 | Yes | No | No | No |
| IFP-100ECS | Yes | No | No | No |
| IFP-1000 | Yes | No | No | No |
| IFP-1000ECS | Yes | No | No | No |
| IFP-2000 | Yes | No | No | No |
| IFP-2000ECS | Yes | No | No | No |



CAUTION: WHEN SUPPORTING THE ALARM TRANSMISSION, IT IS RECOMMENDED THAT THE FARENHYT PANEL SHOULD USE SECONDARY ANN BUS CHANNEL WITH CLASS A WIRING. IF THE ALARM TRANSMISSION SERVICE IS NOT USED, THE PANEL CAN USE EITHER THE PRIMARY OR THE SECONDARY ANN BUS CHANNEL FOR THE CLSS GATEWAY CONNECTION.

Minimum Required Versions

For the CLSS Gateway: 3.1.4.74

C.5.2 To Use an RS-485 Connection

Using an RS-485 cable the CLSS Gateway connects with the annunciator primary terminal of the panel.



CAUTION: CONNECT EITHER THE CLSS GATEWAY OR THE ANN S/P G MODULE WITH THE PANEL. BOTH OF THEM SHOULD NOT BE CONNECTED TOGETHER WITH THE PANEL.

1. On the Gateway Side

At the RS-485 A port in the gateway board:

- Connect the A connector to the IN+ pin of the RS-485 A port.
- Connect the B connector to the IN- pin of the same RS-485 A port.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the [Figure C.2](#).

2. On the Panel Side

At the S-BUS board in the ANN-BUS PRI terminal:

- Connect the RS-485 +ve wire to the A port.
- Connect the RS-485 -ve wire to the B port.

3. Power Connection

On the Gateway Side

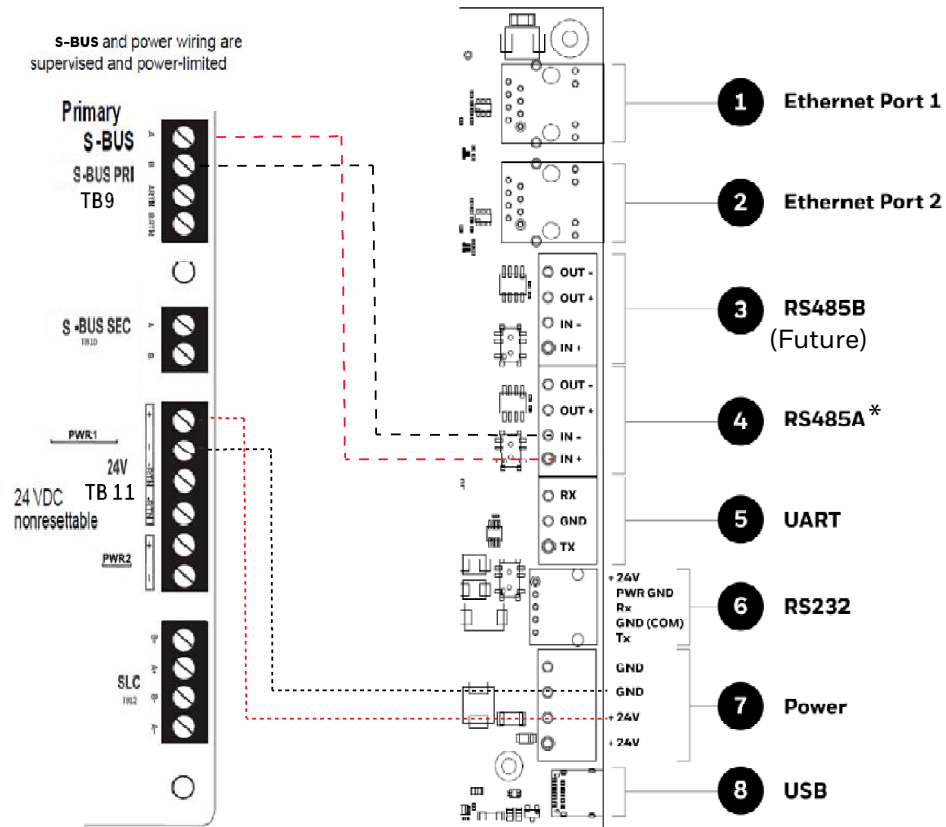
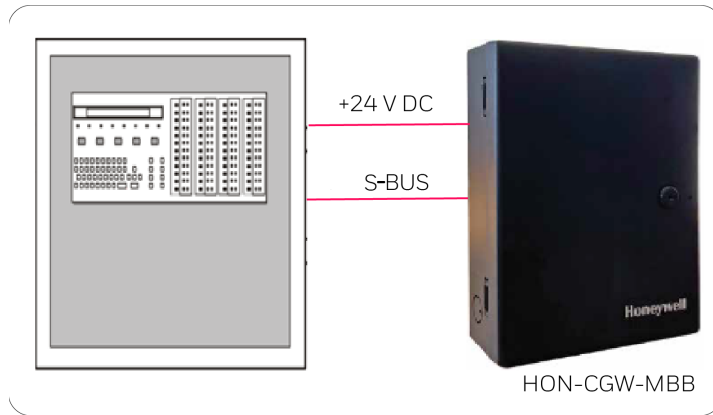
In the power supply port (labeled 7 in the [Figure C.2](#)):

- Connect the Red wire to the +24V pin.
- Connect the Black wire to the Gnd pin.

On the Panel Side

In the power board of the panel:

- Connect the Red wire to the +ve pin.
- Connect the Black wire to the -ve pin.



(* For panel connection, use only the RS-485A port)

Figure C.10: Farenhyt Panel: RS-485 Connections

C.5.3 Programming for Annunciator (ANN-PRI)

Programming enables the panel to recognize the CLSS gateway and the annunciator.



CAUTION: BEFORE PROGRAMMING, ENSURE THAT THE ANN-PRI COMMUNICATION CABLE IS CONNECTED WITH THE PANEL.

C.5.4 To Program for Annunciator

Using the keypad on the panel, you select options on the screens.

1. On the panel, press the **Enter** button on the keypad.
2. View the panel screen options.
3. On the keypad, press **7** to select **7 = PROGRAMMING MODE**.
4. Enter the panel's password in the **PROGRAMMING** screen.
The default password is: 00000000
5. Select the panel connected with the gateway, if it is a standalone panel.

OR

Navigate in the list of panels and select the panel connected with the gateway if it is a multi-panel network.

6. Select **1 = MODULE**.
7. Select **2 = ADD MODULE**.
8. Select the module of the gateway from the list.
9. Select the module type.
10. Select **1 = EDIT MODULE** to enter the module details.
11. Follow the on-screen instructions and enter the communication settings.
12. Review the entered details.

C.6 FireWarden Panels

C.6.1 Connection Options

The gateway operates only with the FireWarden fire alarm control panels as listed in the table below:

Table C.4: FireWarden Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | RS-232 | USB |
|-------------------------|--------|----------|--------|-----|
| FireWarden-50X | Yes | No | No | No |
| FireWarden-100X | Yes | No | No | No |



CAUTION: WHEN SUPPORTING THE ALARM TRANSMISSION, IT IS RECOMMENDED THAT THE FIREWARDEN PANEL SHOULD USE SECONDARY ANN BUS CHANNEL WITH CLASS A WIRING. IF THE ALARM TRANSMISSION SERVICE IS NOT USED, THE PANEL CAN USE EITHER THE PRIMARY OR THE SECONDARY ANN BUS CHANNEL FOR THE CLSS GATEWAY CONNECTION.

Minimum Required Versions

For the Panel: 1.03.006

For the CLSS Gateway: 3.0.3.116

C.6.2 To Use an RS-485 Connection

Using an RS-485 cable the CLSS Gateway connects with the annunciator primary terminal of the panel.



CAUTION: CONNECT EITHER THE CLSS GATEWAY OR THE ANN S/P G MODULE WITH THE PANEL. BOTH OF THEM SHOULD NOT BE CONNECTED TOGETHER WITH THE PANEL.

1. On the Gateway Side

At the RS-485 port in the gateway board:

- Connect the A connector to the IN+ pin of the RS-485 port.
- Connect the B connector to the IN- pin of the same RS-485 port.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the [Figure C.2](#).

2. On the Panel Side

At the TB9 port in the ANN-BUS PRI terminal:

- Connect the RS-485 +ve wire to the A port.
- Connect the RS-485 -ve wire to the B port.

3. Power Connection

On the Gateway Side

In the power supply port (labeled 7 in the [Figure C.2](#)):

- Connect the Red wire to the +24V pin.
- Connect the Black wire to the Gnd pin.

On the Panel Side

In the TB11 port of the panel:

- Connect the Red wire to the +ve pin.
- Connect the Black wire to the -ve pin.

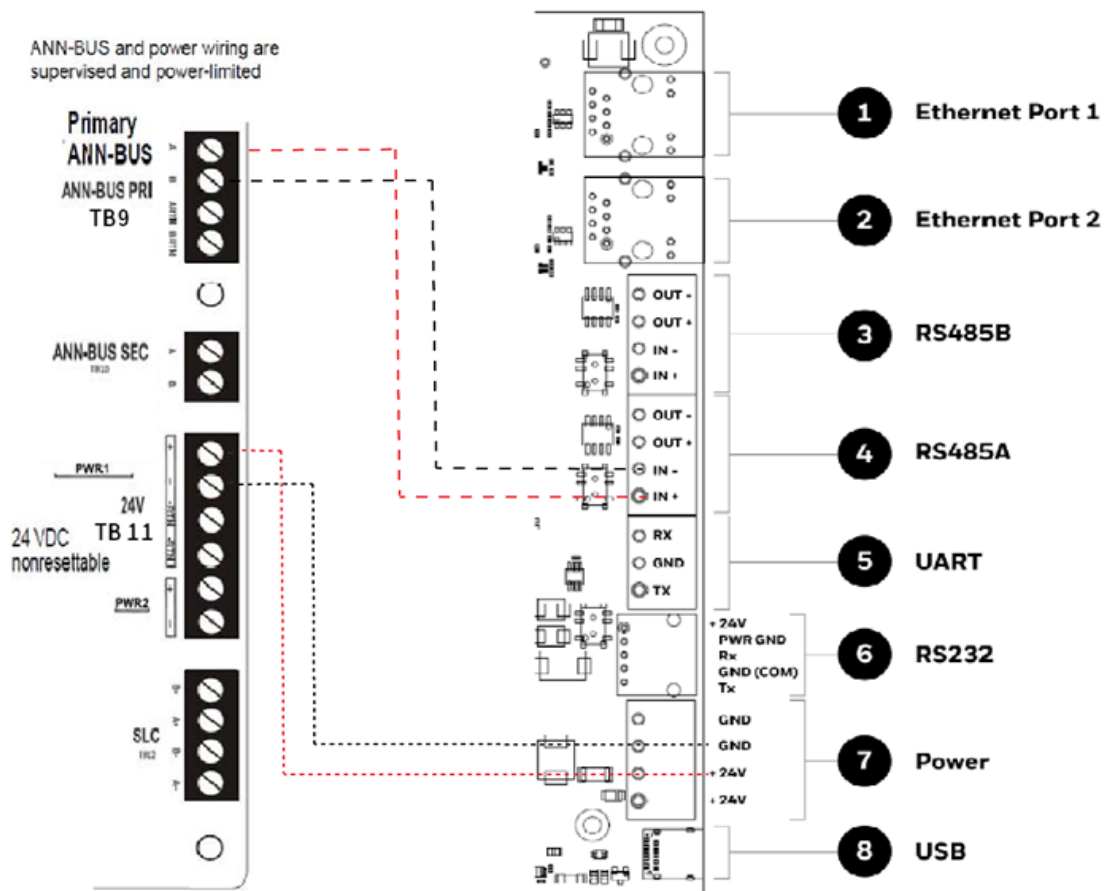
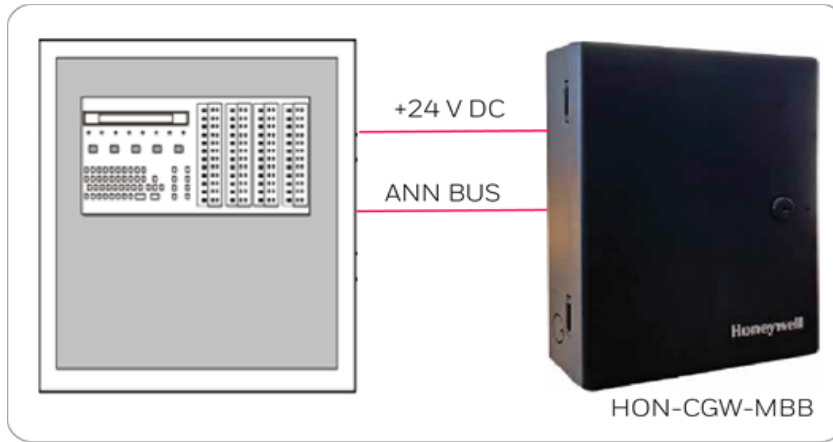


Figure C.11: FireWarden Panel: RS-485 Connections

C.6.3 Programming for Annunciator (ANN-PRI)

Programming enables the panel to recognize the CLSS gateway and the annunciator.



CAUTION: BEFORE PROGRAMMING, ENSURE THAT THE ANN-PRI COMMUNICATION CABLE IS CONNECTED WITH THE PANEL.

C.6.4 To Program for Annunciator

Using the keypad on the panel, you select options on the screens.

1. On the panel, press the **Enter** button on the keypad.
2. View the panel screen options.
3. On the keypad, press **2** to select **2 = PROGRAMMING MODE**.
4. Enter the panel's password in the **PROGRAMMING** screen.
The default password is: 00000000
5. Press the down arrow button to select **2 = POINT PROGRAM**.
6. Select **3 = FUTURE USE** and then select **3 = ANNUNCIATORS**.
7. Select **1 = PRIMARY** on the **ANN-BUS SELECT** screen.
8. Ensure **1 = ENABLED YES** on the **ANN PRIMARY** screen.
9. Select **2 = MODULES INSTALLED**.
10. Select **1 = ADDR. 1-1 NONE** on the **ANN-BUS MODULES** screen.
11. Ensure **1 = TYPE NONE** on the **ANN-BUS MODULE 1-1** screen.
12. Press the down arrow button once to go back to the **ANN-BUS MODULE TYPE** screen.
13. Press the down arrow button to go to the next screen.
14. Select **2 = ANN-S/PG MODULE**.
15. On the keypad, press the **Esc** key three times to go back to the **ANN/BUS SELECT** screen.
16. Select **3 = ANN-BUS OPTIONS**.
17. Press **1 = ANN-S/PG OPTIONS** on the **ANN-BUS** screen.
18. Set **CLASS A** to **YES** if your ANN Bus wiring is Class A topology, otherwise set it as **NO**.
19. Ensure the following settings on the **ANN-S/PG OPTIONS** screen:
 - 1 = PORT PAR**
 - 2 = PRINTER SUPV YES**
 - 3 = OFFLINE TIMER 0**
20. Press the **Esc** button continuously until the main screen appears.
The panel saves the changes and resets.

To Verify the Changes

It is a good practice to confirm that the panel reflects the changes you did.

1. Use the keypad and go to the **ANN-BUS MODULES** screen.
2. Check that **1 = ADDR. 1-1 ANN-S/PG** on the **ANN-BUS MODULE 1-1** screen.
3. Check that no ANN primary fault is reported on the main screen.

C.6.5 To Use Panel's Printer Port Connection

Some FireWarden panels support data transfer through their printer terminal.



NOTE: Compatible CLSS Gateway firmware versions: 2.1.11.16 and above

1. On the Gateway Side

- Connect the serial cable into the RS-232 port of the gateway.
The RS-232 port is labeled as 6 in the [Figure C.13](#).

2. On the Panel Side

Connect the serial cable in the DB9 serial port of the ANN-S/PG module on the panel.



CAUTION: ENSURE THAT ONLY THE ANN-S/PG IS CONNECTED AND NOT THE CLSS GATEWAY. ONLY ONE OF THESE TWO CAN BE CONNECTED. BOTH OF THEM MUST NOT BE CONNECTED TOGETHER.

3. Power Connection

On the Gateway Side

- Connect to the 24V DC external power supply.
- Switch the S7 Switch next to the RS-232 port towards *NUP_OUT*.

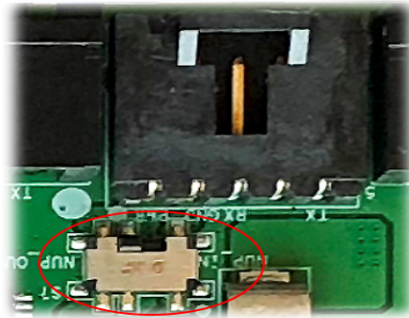


Figure C.12: The S7 Switch

On the Panel Side

Connect the power cable to a 24V DC external power source or the panel's power supply.

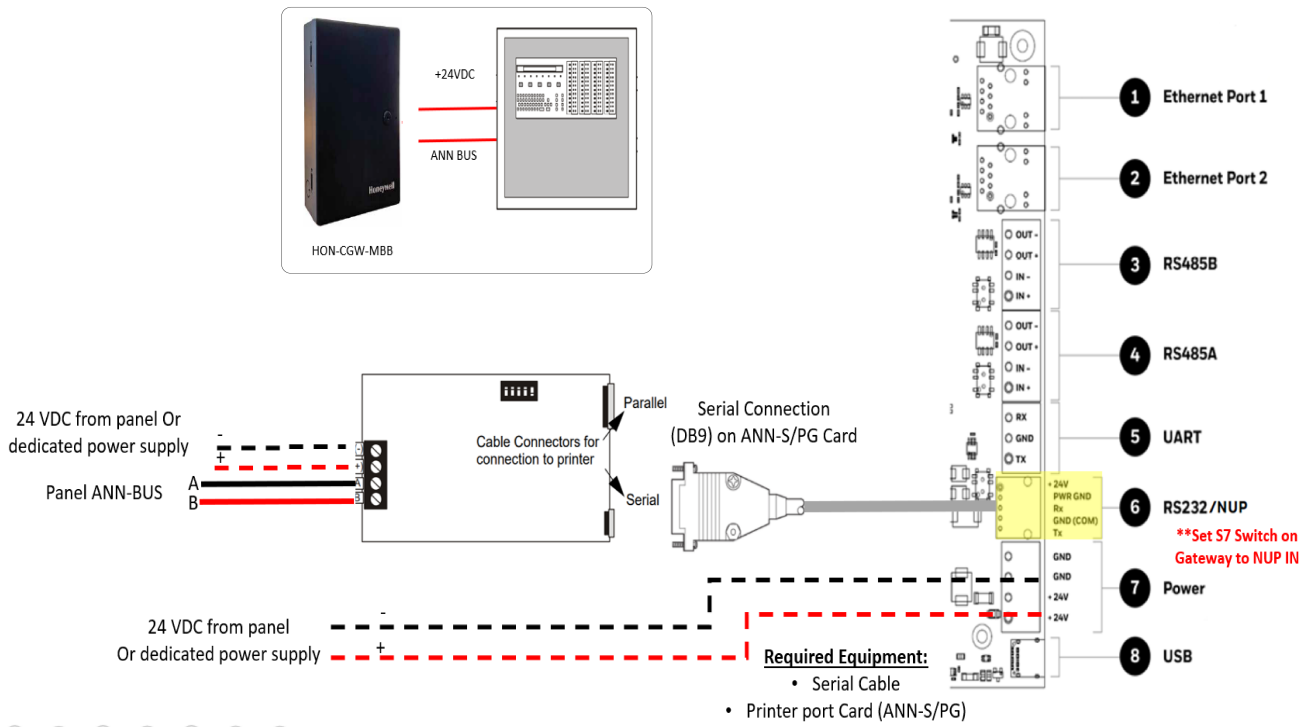


Figure C.13: FireWarden Panels: Printer Port Connections

C.7 Gamewell-FCI Panels

C.7.1 Connection Options

Each variant of the Gamewell-FCI panel offers various connection options. The gateway operates only with the Gamewell-FCI fire alarm control panels listed in the table below:

Table C.5: Gamewell-FCI Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | RS-232 | USB | Ethernet |
|-------------------------|--------|----------|--------|-----|----------|
| E3 Series Panels | | | | | |
| ILI-MB-E3 | Yes | No | No | Yes | No |
| ILI-S-E3 | No | No | No | Yes | No |
| ILI95-MB-E3 | Yes | No | No | Yes | No |
| ILI95-S-E3 | No | No | No | Yes | No |
| S3 Series Panels | | | | | |
| SLP-E3 | Yes | No | No | Yes | Yes |
| INI-7100 | Yes | No | No | Yes | No |



CAUTION: DO NOT INSTALL DACT-E3 AND THE CLSS GATEWAY TOGETHER ON AN ILI-MB-E3 CIRCUIT BOARD OR AN ILI95-MB-E3 CIRCUIT BOARD. YOU CAN USE DACT-E3 ON A DIFFERENT NODE WITHIN THE NETWORK.

Minimum Required Versions

- Gamewell-E3: 7.00.106
- Gamewell-S3: 7.00.106
- CLSS Gateway: 3.1.4.72
- LCD-SLP (Display Panel): 2.12.090
- NGA-K: 7.00.100

Limitation(s)

Support for CAM-event alerts is *currently* not available for the *CLSS Gateway*. When the support is available, the *CLSS Gateway* will send these messages to *CLSS Site Manager* (Cloud) and the *CLSS App*.

C.7.2 To Use Panel’s Printer Port Connection

Gamewell panels support data transfer through their RS-485 connection. The transferred data is stored in the *CLSS Site Manager*.

1. On the Gateway Side

1. Connect the + (24 V) wire to the IN+ pin of an RS-485 port.
2. Connect the - (GND) wire to the IN- pin of an RS-485 port.

The RS-485 ports are labeled as 3 and 4 in the [Figure C.13](#).

2. On the Panel Side

- [E3 Series Panel](#)
- [S3 Series Panel](#)
- **E3 Series Panel**

At the TB3 terminal of the panel,

- Connect the +ve wire to the TB3-1 pin.
- Connect the -ve wire to the TB3-2 pin.

At the TB6 terminal of the panel,

- Connect the GND wire to the TB6-1 pin.
- Connect the TxD wire to the TB6-2 pin.
- Connect the SUPV wire to the TB6-3 pin.

- Connect the RxD wire to the TB6-4 pin.

Power Connection

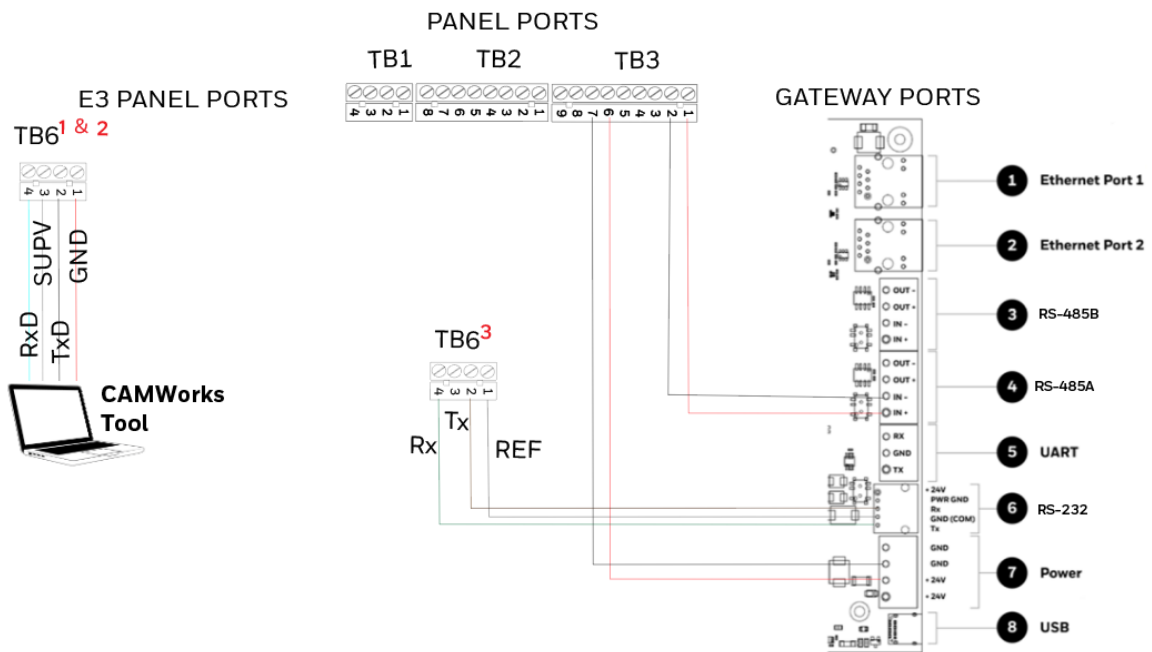
On the Gateway Side

Ensure that the power cable is connected with the power port of the gateway.

The power port is labeled as 7 in the [Figure C.13](#).

On the Panel Side

- Connect the Red wire to the +ve pin in the TB3 port.
- Connect the Black wire to the -ve pin in the TB3 port.



- 1 Disconnect the CAMWorks Tool after downloading the configuration file. Then, connect RS-232 to TB6 for Control Functionality.
- 2 If the computer has a serial port, connect it with the RS-232 to DB9 converter (P/N: 75267). If the computer does not have a serial port, connect the converter with the USB port of the computer.
- 3 Control Functionality

Figure C.14: E3 Panel: Gateway Connections

TB6 and RS-232 Connections

The pin connections are as below:

| TB6 Pins | RS-232 Pins | Description |
|----------|--------------------|--|
| TB6-1 | RS-232 GND | <i>For Programming.</i> GND connects to the Red lead on the download cable of P/N 75267. For Printer port, GND connects to printer DB-9 and PIN-5. |
| TB6-2 | RS-232 TxD | <i>For Programming.</i> TxD connects to the Black lead on the download cable of P/N 75267. For Printer port, TxD connects to printer DB-9 and PIN-2. |
| TB6-3 | RS-232 Supervision | For optional printer supervision. For Printer port, SUPV connects to printer DB-9 and PIN-4. |
| TB6-4 | RS-232 RxD | <i>For Programming.</i> RxD connects to the Green lead on the download cable of P/N 75267. For Printer port, RxD connects to printer DB-9 and PIN-3. |

- **S3 Series Panel**

At the TB3 terminal of the panel,

- Connect the +ve wire to the TB3-1 pin.
- Connect the -ve wire to the TB3-2 pin.

At the TB5 terminal of the panel,

- Connect the GND wire to the TB5-1 pin.
- Connect the TxD wire to the TB5-2 pin.
- Connect the SUPV wire to the TB5-3 pin.
- Connect the RxD wire to the TB5-4 pin.

Power Connection

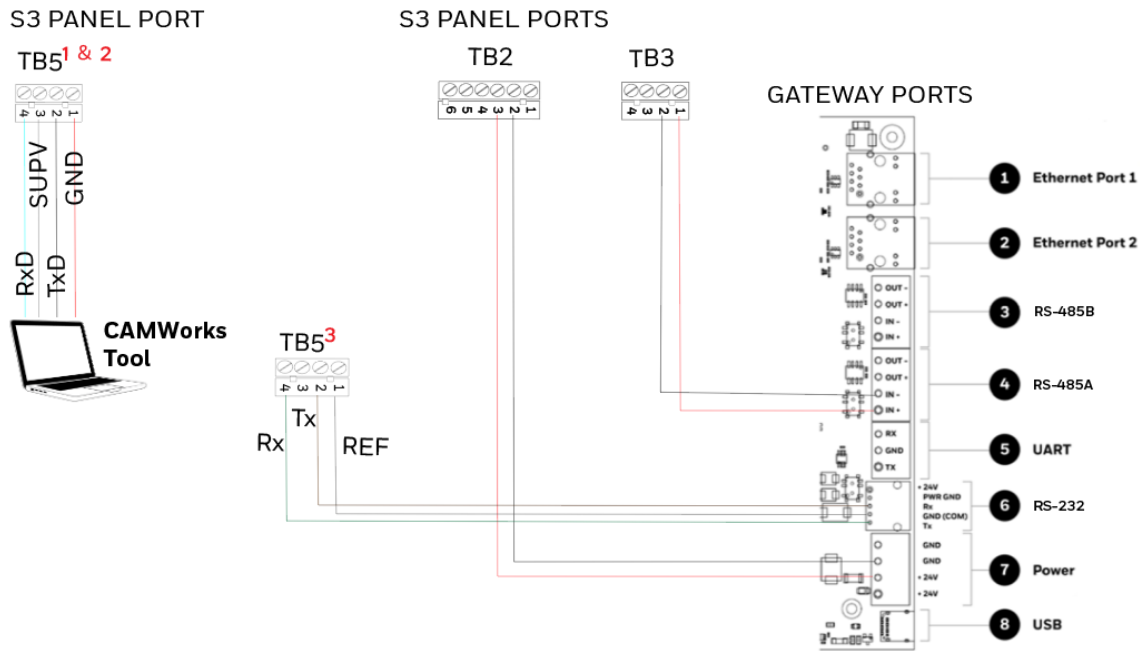
On the Gateway Side

Ensure that the power cable is connected with the power port of the gateway.

The power port is labeled as 7 in the [Figure C.13](#).

On the Panel Side

- Connect the Red wire to the +ve pin in the TB2 port.
- Connect the Black wire to the -ve pin in the TB2 port.



- 1 Disconnect the CAMWorks Tool after downloading the configuration file. Then, connect RS-232 to TB5 for Control Functionality.
- 2 If the computer has a serial port, connect it with the RS-232 to DB9 converter (P/N: 75267). If the computer does not have a serial port, connect the converter with the USB port of the computer.
- 3 Control Functionality

Figure C.15: S3 Series: Gateway Connections

TB5 and RS-232 Connections

The pin connections are as below:

| TB5 Pins | RS-232 Pins | Description |
|----------|--------------------|--|
| TB5-1 | RS-232 GND | <i>For Programming.</i> GND connects to the Red lead on the download cable of P/N 75267. For Printer port, GND connects to printer DB-9 and PIN-5. |
| TB5-2 | RS-232 Tx | <i>For Programming.</i> Tx connects to the Black lead on the download cable of P/N 75267. For Printer port, Tx connects to printer DB-9 and PIN-2. |
| TB5-3 | RS-232 Supervision | For optional printer supervision. For Printer port, SUPV connects to printer DB-9 and PIN-4. |
| TB5-4 | RS-232 Rx | <i>For Programming.</i> Rx connects to the Green lead on the download cable of P/N 75267. For Printer port, Rx connects to printer DB-9 and PIN-3. |

C.8 Gent Panels

C.8.1 Connection Options

The gateway operates only with the Gent fire alarm control panels as listed in the table below:

Table C.6: Gent Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | RS-232 | USB |
|-------------------------|--------|----------|------------------|-----|
| COMPACT-24-N | No | No | Yes | Yes |
| COMPACT-PLUS | No | No | Yes | Yes |
| VIGPLUS-24 | No | Yes | Yes ¹ | Yes |
| VIGPLUS-72 | No | Yes | Yes ¹ | Yes |
| VIG1-24 | No | Yes | Yes ¹ | Yes |
| VIG1-72 | No | Yes | Yes ¹ | Yes |

¹ Use the add-on I/O card (VIG-IOC-DOM) on the panel.



NOTE: The add-on I/O card (VIG-IOC-DOM) is ordered separately.

C.8.2 Compact Series Panels

For a fixed gateway we recommend using the RS-232 connection. For a portable gateway, we recommend using the USB connection.

To Use a RS-232 Connection

Certain Gent panel variants can directly communicate through the RS-232 connection.

1. On the Gateway Side

Connect the RS-232 cable with pre-formed connector to the RS-232 port of the gateway board.

The RS-232 port is labeled as 6 in the [Figure C.2](#).

2. On the Panel Side

- The baud rate should be 19200.

At the PB6 terminal of the panel,

- Connect the White wire to a Rx1 or Rx2 pin.
- Connect the Brown wire to a Tx1 or Tx2 pin.
- Connect the Green wire to the 0V pin.



NOTE: Connect either the Tx1 and Rx1 or the Tx2 and Rx2.



NOTE: If Tx1 and Rx1 are connected, select the Port 1 settings in the panel for communication. If Tx2 and Rx2 are connected, select the Port 2 settings in the panel for communication.

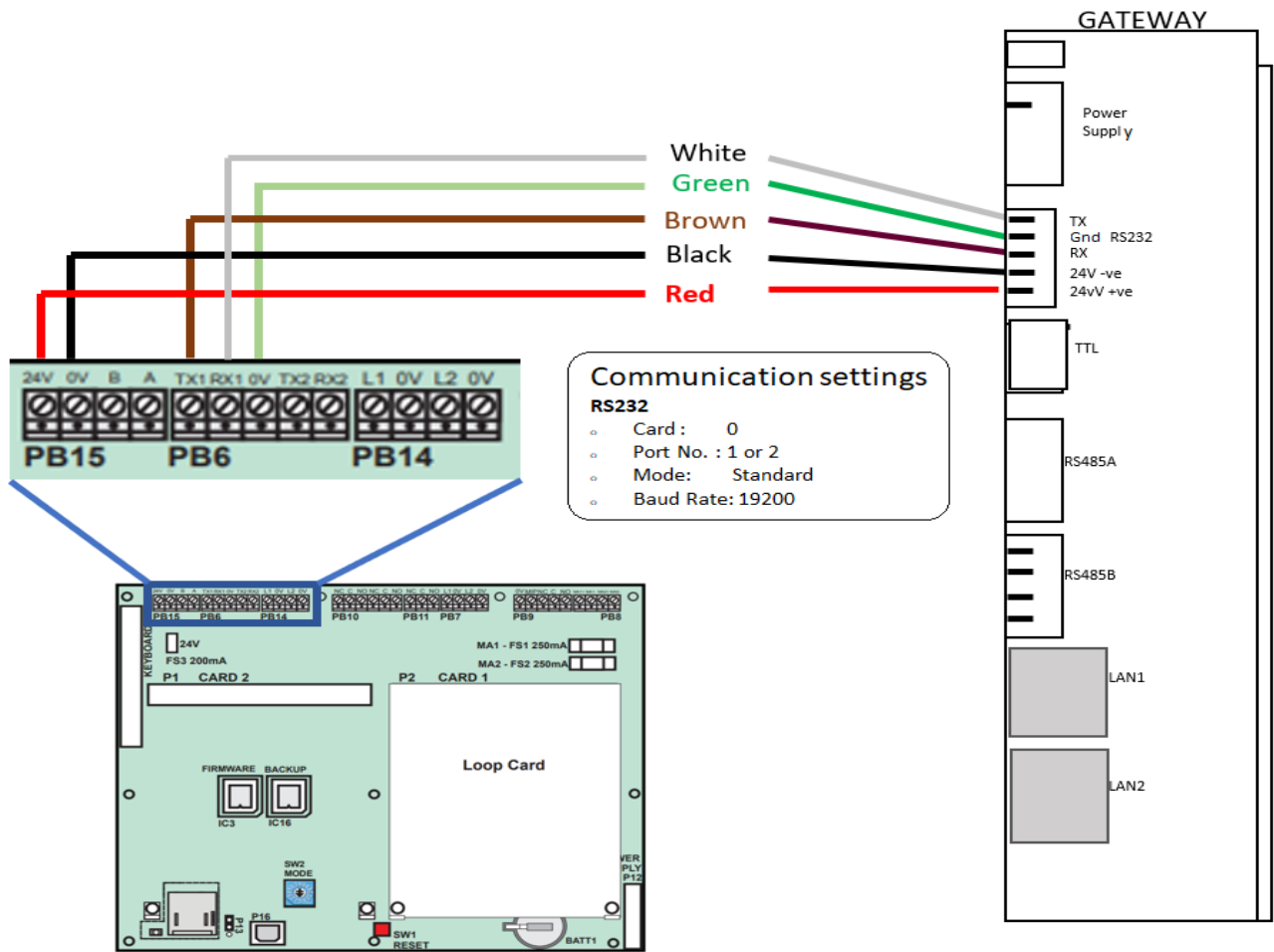


Figure C.16: COMPACT Panels: RS-232 Connections on the PB6 Terminal

3. Power Connection

On the Gateway Side

1. Ensure that the RS-232 cable is connected with the RS-232 port of the gateway.
2. Ensure that the S7 switch next to the RS-232 port is switched towards NUP_IN.

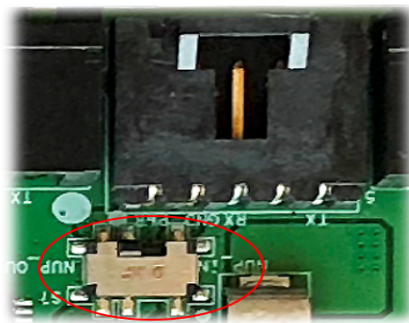


Figure C.17: The S7 Switch

On the Panel Side

At the PB15 terminal of the panel,

- Connect the Red wire (+ve) to the +24V pin.
- Connect the Black wire (-ve) to the 0V pin.

To Use a USB Connection

1. On the Gateway Side

Connect the USB-C side of the cable to the USB port of the gateway.
The USB port is labeled as 8 in the figure [Figure C.2](#).

2. On the Panel Side

Connect the USB-B side of the cable to the USB port of the panel.

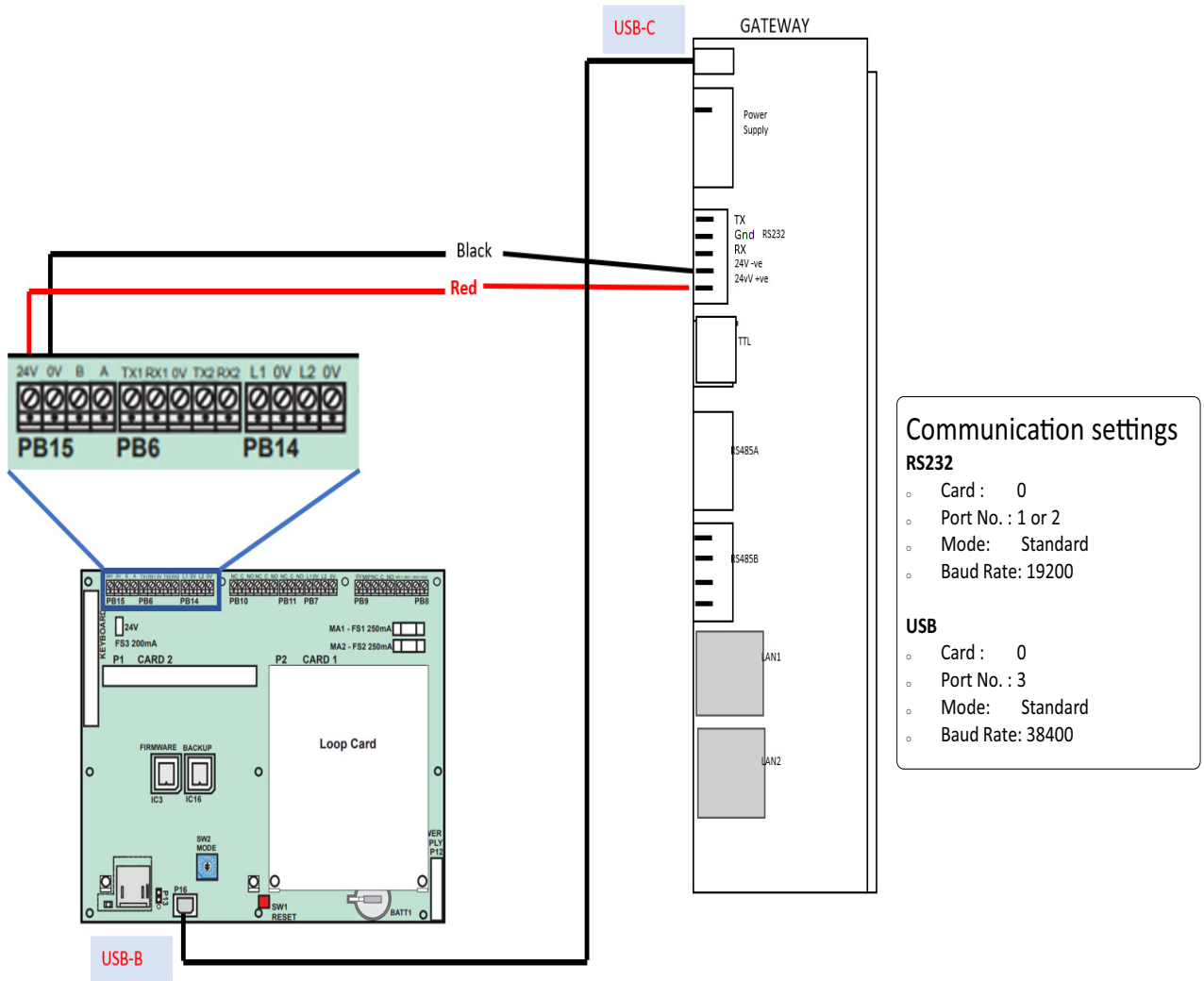


Figure C.18: Compact Panels: USB Connection

3. Power Connection

In the PB15 terminal on the panel,
Connect the gateway to a 24V DC internal power source of the panel.



NOTE: The external power supply must be dedicated and not shared with any other devices.



NOTE: The panel's power supply to the gateway must be within +24V DC power.

C.8.3 Vigilon Series Panels

For a fixed gateway, we recommend using a UART/TTL connection. If it is not available, use a RS-232 connection.

To Use a UART/TTL Connection

1. On the Gateway Side

Connect the male UART/TTL cable to the Rx (Red), Gnd (Silver), and Tx (White) UART/TTL terminals of the gateway.

The UART/TTL port is labeled as 5 in [Figure C.2](#).

2. On the Panel Side

1. Within the panel, find the backplane PCB board (see [Figure C.19](#)).
2. Connect the 3.5mm phono socket to the P11 connector on the panel's PCB.

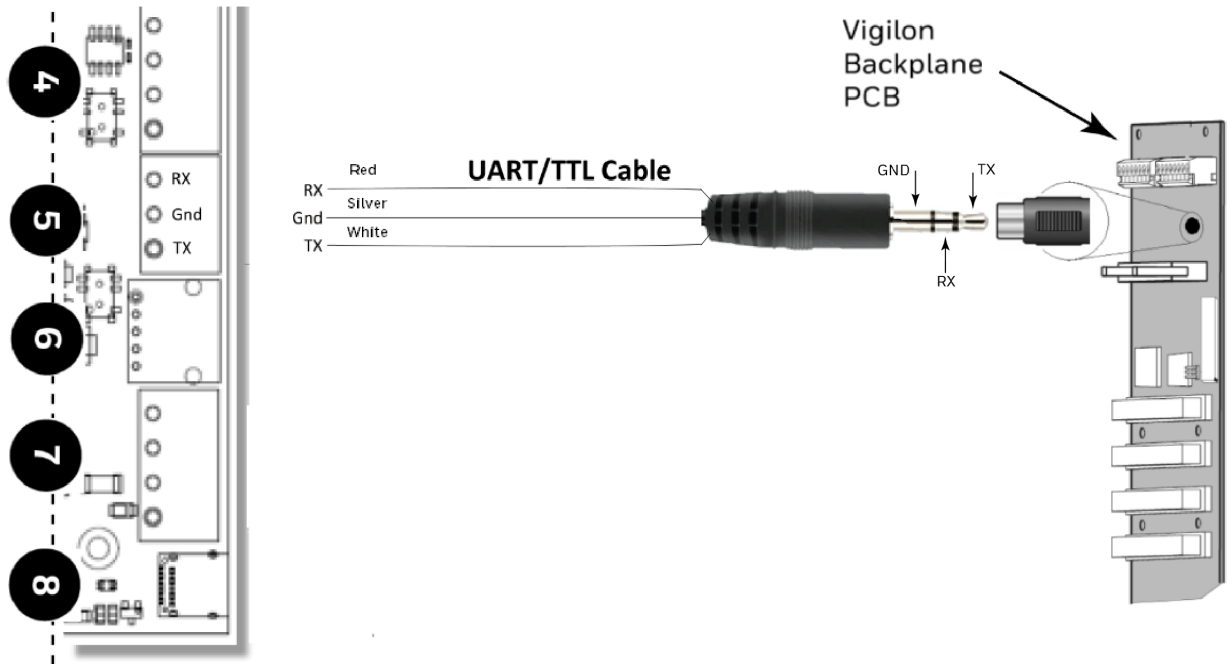


Figure C.19: Vigilon Panels: UART/TTL Connection

3. Power Connection

On the Gateway Side

Connect the power cable to a 24V DC external power source.



NOTE: The external power supply must be dedicated and not shared with any other devices.



NOTE: The panel's power supply to the gateway must be within +24V DC power.

To Use an RS-232 Port via an I/O Card

Using an add-on I/O card (VIG-IOC-DOM), certain Vigilon panel variants can communicate with the CLSS Gateway.

- The I/O card has a rotary switch, which should point to 5.
- The baud rate of the I/O card should be 19200.

1. On the Gateway Side

1. Connect the RS-232 cable to the RS-232 port of the gateway.

The RS-232 port is labeled as 6 in the [Figure C.2](#).

2. On the Panel Side

1. Inside the panel enclosure, find the backplane PCB board.
2. Insert the I/O card into the P2 Card 15.

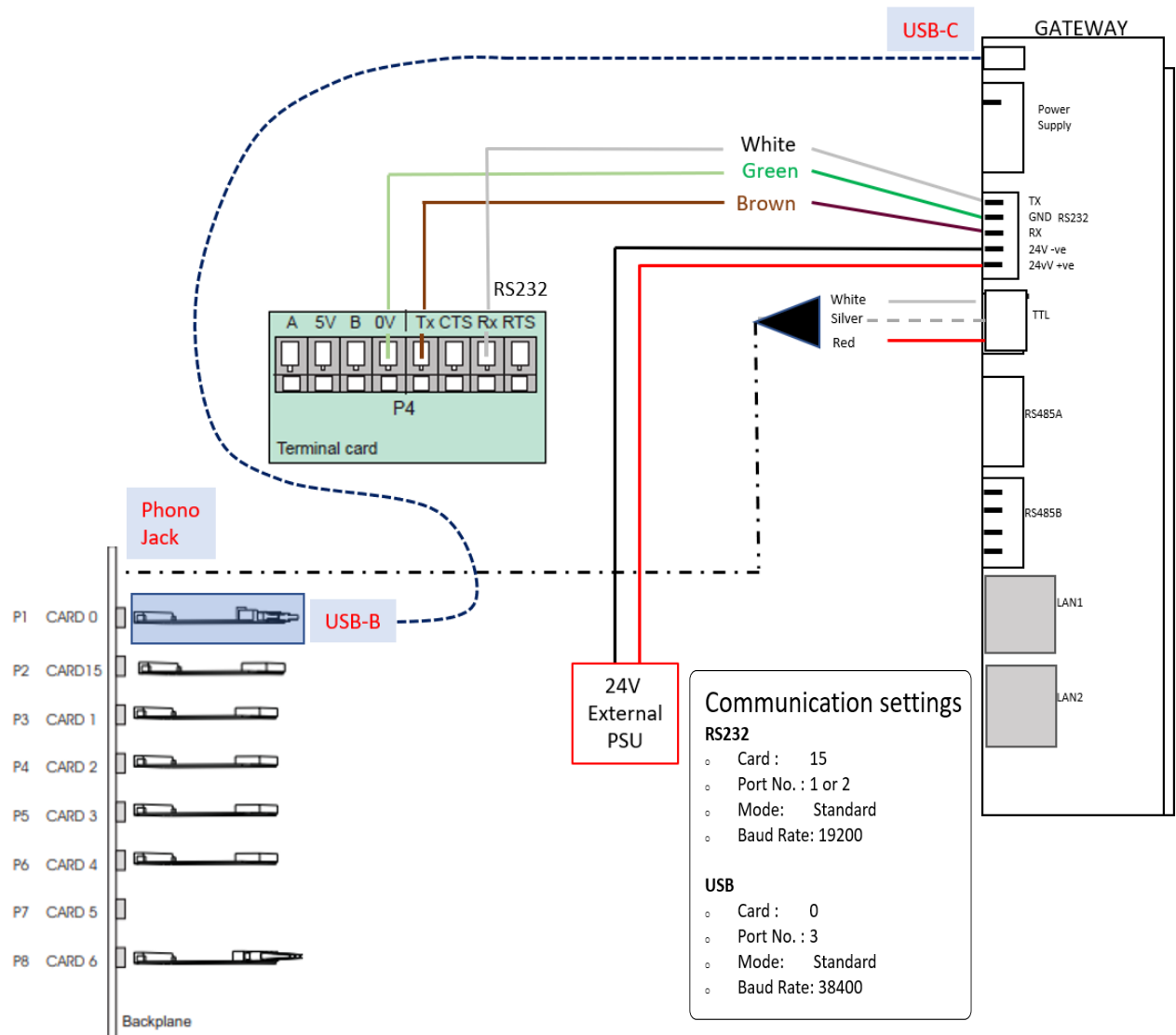


Figure C.20: Vigilon Panels: I/O Card Connection

For the P2 Card 15-Connected I/O Card:

1. In the panel, find the RS-485/RS-232 (P4) connectors on the main control board.
2. Connect the RS-232 cable to the Tx (Brown), Rx (White), and 0V (Green) terminals of the RS-485/RS-232 (P4) connectors.

3. Power Connection



NOTE: The external power supply must be dedicated and not shared with any other devices.



NOTE: The panel's power supply to the gateway must be within +24V DC power.

On the Gateway Side

1. Connect to the 24V DC external power supply.
2. Ensure that the S7 switch next to the RS-232 port is switched towards *NUP_OUT*.

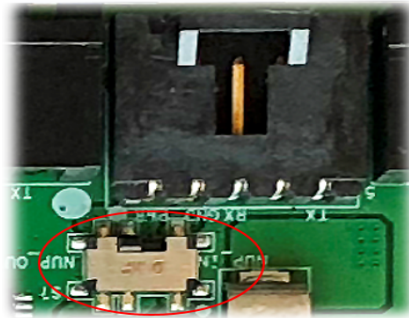


Figure C.21: The S7 Switch

On the Panel Side

Connect the power cable into the 24V DC external power supply.

To Use a USB Connection

1. On the Gateway Side

Connect the USB-C side of the cable to the USB port of the gateway. The USB port is labeled as 8 in the figure [Figure C.2](#).

2. On the Panel Side

In the MCC card on the panel:

Connect the USB-B side of the cable. Refer to the figure [Figure C.20](#).

3. Power Connection

Connect the gateway to a 24V DC external power source.



NOTE: The external power supply must be dedicated and not shared with any other devices.



NOTE: The panel's power supply to the gateway must be within +24V DC power.

C.9 Morley-IAS Panels

C.9.1 Connection Options

The gateway operates only with the Morley-IAS fire alarm control panels listed in the table below:

Table C.7: Morley-IAS European Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | RS-232 | USB |
|-------------------------|--------|----------|------------------|-----|
| DXc | No | No | Yes ¹ | No |

1 Use the serial communication card (P/N: 795-122) on the panel.



NOTE: Compatible CLSS Gateway firmware versions: 3.0.2.30 and above.

C.9.2 To Use an RS-232 Connection

Morley-IAS panel variants use an RS-232 connection with the CLSS Gateway.

1. On the Gateway Side

1. Connect the RS-232 cable with pre-formed connector to the RS-232 port of the gateway board.

The RS-232 port is labeled as 6 in the [Figure C.2](#).

2. On the Panel Side

- [Morley DXc Panels](#)



NOTE: In a network of panels, connect the gateway to the master panel.

• Morley DXc Panels

In the SK1 terminal of the panel:

- Connect the White wire to the RxD+ pin.
- Connect the Green wire to the Gnd pin.
- Connect the Brown wire to the TxD+ pin.

3. Power Connection

The gateway's RS-232 port can receive its power either from an external power source or from the non-resettable internal power of the panel.



NOTE: The external power supply must be dedicated and not shared with any other devices.



NOTE: The panel's power supply to the gateway must be within +24V DC power.

For the External Power Supply:

On the Gateway Side

1. Connect to the 24V DC external power supply or to the panel's 24V DC power port.
2. Ensure that the S7 switch next to the RS-232 port is switched towards *NUP_OUT*.

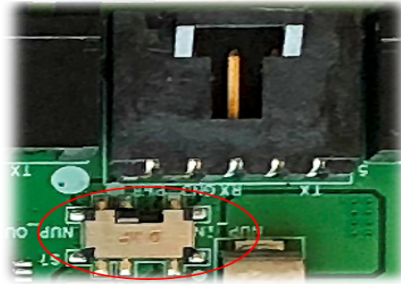


Figure C.22: The S7 Switch

On the Panel Side

In the SK4 or SK5 terminal,

Connect the RS-232 cable for the non-resettable internal power.

C.10 NOTIFIER® UL

C.10.1 Connection Options

The gateway operates only with the NOTIFIER fire alarm control panels as listed in the table below:

Table C.8: NOTIFIER UL Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | NUP | USB |
|-------------------------|--------|----------|-----|-----|
| ONYX Panels | | | | |
| NFS-320 | No | No | Yes | No |
| NFS2-640 | No | No | Yes | No |
| NFS2-3030 | No | No | Yes | No |
| INSPIRE Panels | | | | |
| N16E | No | No | Yes | No |
| N16X | No | No | Yes | No |

C.10.2 To Use a NUP Connection

Some NOTIFIER panel variants use a NUP connection with the CLSS Gateway.

1. On the Gateway Side

Connect the NUP cable to the NUP port of the gateway board.

The NUP port is labeled as 6 in the [Figure C.23](#).

2. On the Panel Side

In the NUP socket of the panel:

- Stand-alone Panel: Connect the NUP cable.

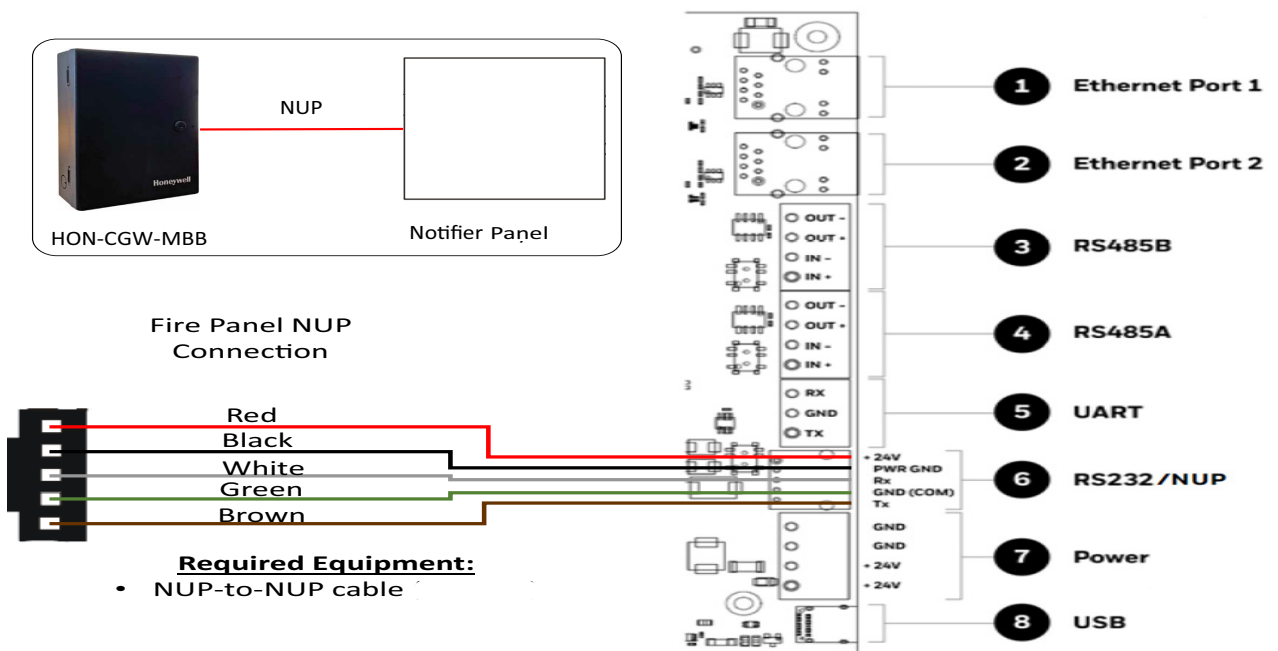


Figure C.23: Stand-alone Panel: NUP Connection

- Standard-speed Network of Panels: Add an additional standard NCM card to the panel for the gateway connection.



NOTE: For the standard-speed network, each device should have its NCM card on the panel with an available port.

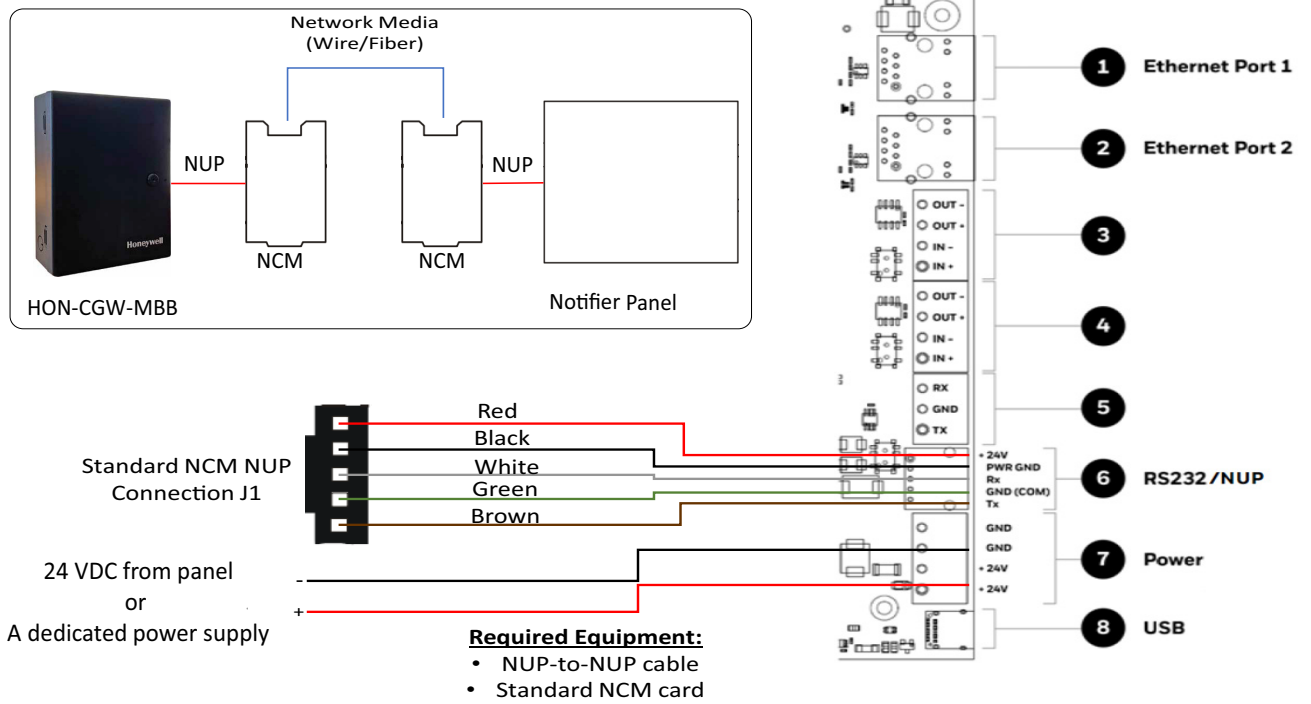


Figure C.24: Standard-speed Network Panel: NUP Connection

- High-speed Network of Panels: Connect the NUP cable into an open NUP port of the HS-NCM card on the panel. If no NUP port is available, an additional HS-NCM card must be added and connected.

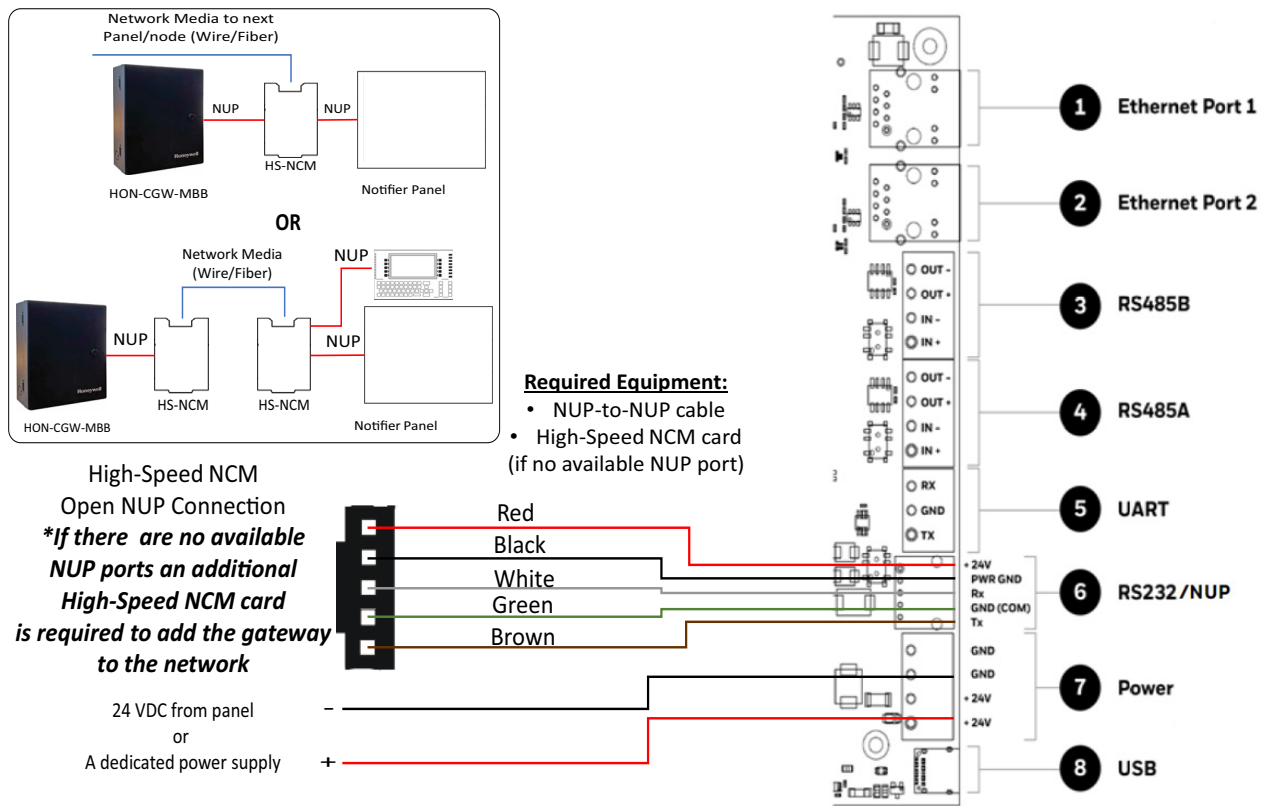


Figure C.25: High-speed Network Panel: NUP Connection

3. Power Connection



NOTE: The external power supply must be dedicated and not shared with any other devices.



NOTE: The panel’s power supply to the gateway must be within +24V DC power.

On the Gateway Side

- Stand-alone Panel:
 - Ensure that the NUP cable is connected with the NUP port of the gateway.
 - Find the S7 switch next to the NUP port, and switch it towards *NUP_IN*.

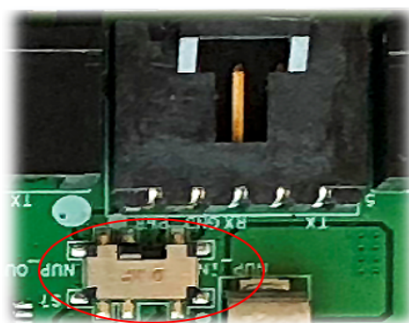


Figure C.26: The S7 Switch

- High-speed or standard-speed network of panels:
 - Connect to the +24V external power source or to the internal power supply of the panel.
 - To power the HS-NCM or NCM over NUP from the gateway:
Find the S7 switch next to the NUP port, and switch it towards *NUP_OUT*.

On the Panel Side

- Stand-alone Panel: Ensure that the NUP cable is connected with the NUP port (J1) of the panel.
- Network of Panels: Connect to a +24V external power source or to the panel's power supply port.

C.11 NOTIFIER® European Panels (EN)

C.11.1 Connection Options

The gateway operates only with the NOTIFIER fire alarm control panels listed in the table below:

Table C.9: NOTIFIER European Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | NUP (RS-232) | USB |
|------------------------------|--------|----------|-----------------------|-----|
| INSPIRE Fusion Panels | | | | |
| E10 | No | No | Yes ^{1 or 2} | No |
| E15 | No | No | Yes ^{3 or 4} | No |

- 1 Use the serial communication card (P/N: HOP-405-100) on the panel.
- 2 Use the I/O card (P/N: HOP-404-100) on the panel.



NOTE: Compatible CLSS Gateway firmware versions: 3.0.2.30 and above.

C.11.2 Preparing for Connections

For INPIRE panel power connection, you can use either a serial card or an I/O card.

- Configure the serial card or the I/O card for the power connection at the Serial Communication screen of the CLSS Fusion Tool Suite.
- Configure the communication settings at the Serial Communication screen of the CLSS Fusion Tool Suite.

C.11.3 To Use a NUP Connection

Some NOTIFIER panel variants use a NUP connection with the CLSS Gateway.

1. On the Gateway Side

Connect the NUP cable with a pre-formed connector to the NUP port of the gateway board.

Refer to [Figure C.2](#) where the NUP port is labeled as 6. It is the P7 pin on the gateway board.

2. On the Panel Side

- [INSPIRE Panels](#)
- **INSPIRE Panels**

In the serial communication card on the panel:

- Connect the White wire to the pin 9 (CH2 RX/B).
- Connect the Green wire to the pin 8 (CH2 ISO GND).
- Connect the Brown wire to the pin 10 (CH2 TX/A).

3. Power Connection

The gateway can receive its power either from an external power source or from the non-resettable internal power of the panel. For the External Power Supply:



NOTE: The external power supply must be dedicated and not shared with any other devices.



NOTE: The panel's power supply to the gateway must be within +24V DC power.

On the Gateway Side

1. Connect to the 24V DC external power supply or to the panel's 24V DC power port.
2. Ensure that the S7 switch next to the RS-232 port is switched towards *NUP_OUT*.

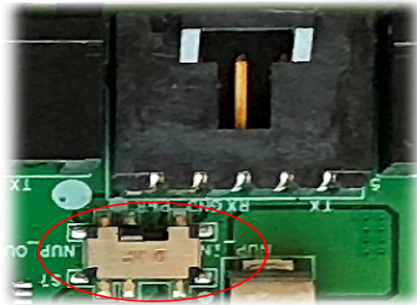


Figure C.27: The S7 Switch

On the Panel Side

- INSPIRE Panels: In the serial communication card or in the I/O card,
 - Connect the Red wire to the pin 1 (Aux. DC OUT +24V).
 - Connect the Black wire to the pin 2 (Aux. DC OUT GND).

External Power Supply

Use this option if the gateway is *not* receiving the power from the panel.

- On the Gateway Side

Connect to the power port of the gateway.

Refer to [Figure C.2](#) where the power port on the gateway is labeled as 7. It is the P2 pin on the gateway board.

- On the External Power Supply Side

Connect to the 24V DC external power supply.

C.12 Silent Knight Panels

C.12.1 Connection Options

The gateway operates only with the Silent Knight fire alarm control panels as listed in the table below:

Table C.10: Silent Knight Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | RS-232 | USB |
|-------------------------|--------|----------|--------|-----|
| 006700 | Yes | No | No | No |
| 006808 | Yes | No | No | No |
| 6820 | Yes | No | No | No |
| 6820EVS | Yes | No | No | No |



CAUTION: WHEN SUPPORTING THE ALARM TRANSMISSION, IT IS RECOMMENDED THAT THE SILENT KNIGHT PANEL SHOULD USE SECONDARY ANN BUS CHANNEL WITH CLASS A WIRING. IF THE ALARM TRANSMISSION SERVICE IS NOT USED, THE PANEL CAN USE EITHER THE PRIMARY OR THE SECONDARY ANN BUS CHANNEL FOR THE CLSS GATEWAY CONNECTION.

Minimum Required Versions

For the Panel: 6.05.01

For the CLSS Gateway: 3.1.4.74

C.12.2 To Use an RS-485 Connection

Using an RS-485 cable the CLSS Gateway connects with the annunciator primary terminal of the panel.



CAUTION: CONNECT EITHER THE CLSS GATEWAY OR THE ANN S/P G MODULE WITH THE PANEL. BOTH OF THEM SHOULD NOT BE CONNECTED TOGETHER WITH THE PANEL.

1. On the Gateway Side

At the RS-485 A port in the gateway board:

- Connect the A connector to the IN+ pin of the RS-485 A port.
- Connect the B connector to the IN- pin of the same RS-485 A port.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the [Figure C.2](#).

2. On the Panel Side

At the S-BUS board in the ANN-BUS PRI terminal:

- Connect the RS-485 +ve wire to the A port.
- Connect the RS-485 -ve wire to the B port.

3. Power Connection

On the Gateway Side

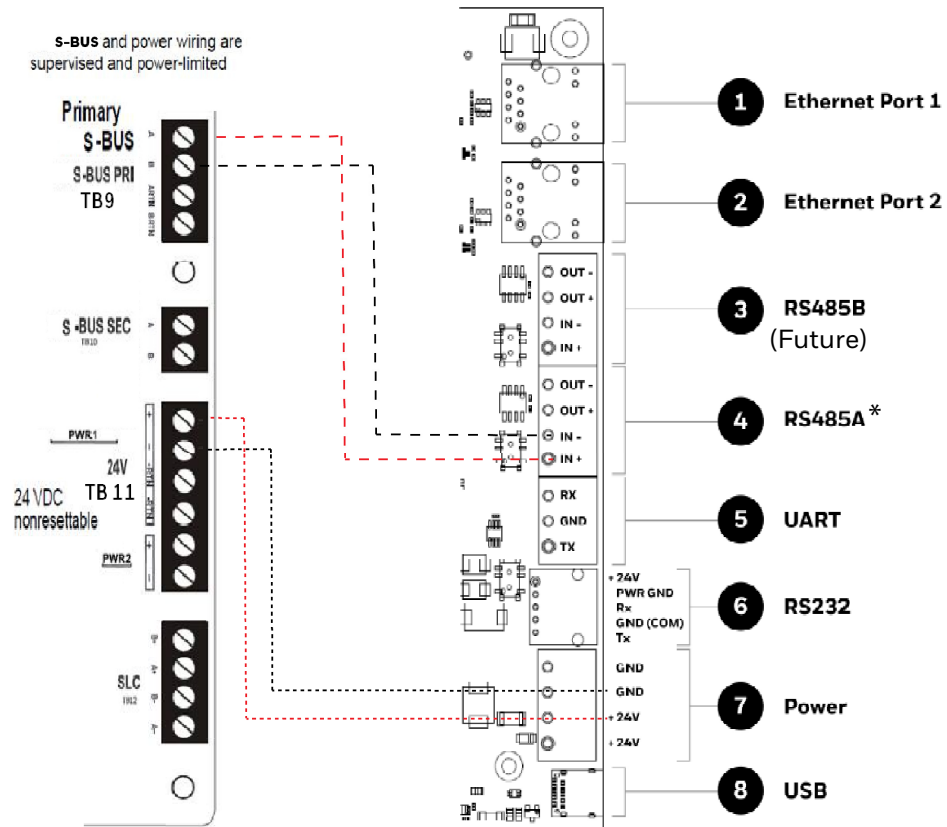
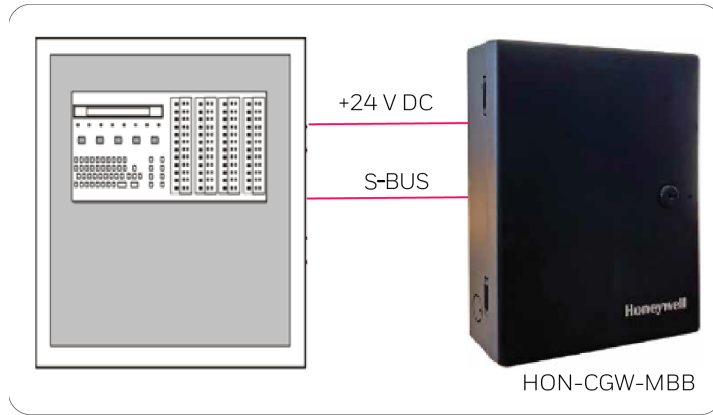
In the power supply port (labeled 7 in the [Figure C.2](#)):

- Connect the Red wire to the +24V pin.
- Connect the Black wire to the Gnd pin.

On the Panel Side

In the power board of the panel:

- Connect the Red wire to the +ve pin.
- Connect the Black wire to the -ve pin.



(* For panel connection, use only the RS-485A port)

Figure C.28: Silent Knight Panel: RS-485 Connections

C.12.3 Programming for Annunciator (ANN-PRI)

Programming enables the panel to recognize the CLSS gateway and the annunciator.



CAUTION: BEFORE PROGRAMMING, ENSURE THAT THE ANN-PRI COMMUNICATION CABLE IS CONNECTED WITH THE PANEL.

C.12.4 To Program for Annunciator

Using the keypad on the panel, you select options on the screens.

1. On the panel, press the **Enter** button on the keypad.
2. View the panel screen options.
3. On the keypad, press **7** to select **7 = PROGRAMMING MODE**.
4. Enter the panel's password in the **PROGRAMMING** screen.
The default password is: 00000000
5. Select the panel connected with the gateway, if it is a standalone panel.

OR

Navigate in the list of panels and select the panel connected with the gateway if it is a multi-panel network.

6. Select **1 = MODULE**.
7. Select **2 = ADD MODULE**.
8. Select the module of the gateway from the list.
9. Select the module type.
10. Select **1 = EDIT MODULE** to enter the module details.
11. Follow the on-screen instructions and enter the communication settings.
12. Review the entered details.

C.13 Triga Panels

C.13.1 Connection Options

The gateway operates only with the Triga fire alarm control panels as listed in the table below:

Table C.11: Triga Panel Connection Options

| Fire Alarm Panel Models | RS-485 | UART/TTL | RS-232 | USB |
|-------------------------|--------|----------|--------|-----|
| TR-75R | Yes | No | No | No |
| TR-75B | Yes | No | No | No |
| TR-2100R | Yes | No | No | No |
| TR-2100B | Yes | No | No | No |
| TR-R2100R | Yes | No | No | No |
| TR-R2100B | Yes | No | No | No |
| TR-2100ECSR | Yes | No | No | No |
| TR-2100ECSB | Yes | No | No | No |



CAUTION: WHEN SUPPORTING THE ALARM TRANSMISSION, IT IS RECOMMENDED THAT THE TRIGA PANEL SHOULD USE SECONDARY ANN BUS CHANNEL WITH CLASS A WIRING. IF THE ALARM TRANSMISSION SERVICE IS NOT USED, THE PANEL CAN USE EITHER THE PRIMARY OR THE SECONDARY ANN BUS CHANNEL FOR THE CLSS GATEWAY CONNECTION.

Minimum Required Versions

For the Panel: 6.05.01

For the CLSS Gateway: 3.1.4.74

C.13.2 To Use an RS-485 Connection

Using an RS-485 cable the CLSS Gateway connects with the annunciator primary terminal of the panel.



CAUTION: CONNECT EITHER THE CLSS GATEWAY OR THE ANN S/P G MODULE WITH THE PANEL. BOTH OF THEM SHOULD NOT BE CONNECTED TOGETHER WITH THE PANEL.

1. On the Gateway Side

At the RS-485 A port in the gateway board:

- Connect the A connector to the IN+ pin of the RS-485 A port.
- Connect the B connector to the IN- pin of the same RS-485 A port.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the [Figure C.2](#).

2. On the Panel Side

At the S-BUS board in the ANN-BUS PRI terminal:

- Connect the RS-485 +ve wire to the A port.
- Connect the RS-485 -ve wire to the B port.

3. Power Connection

On the Gateway Side

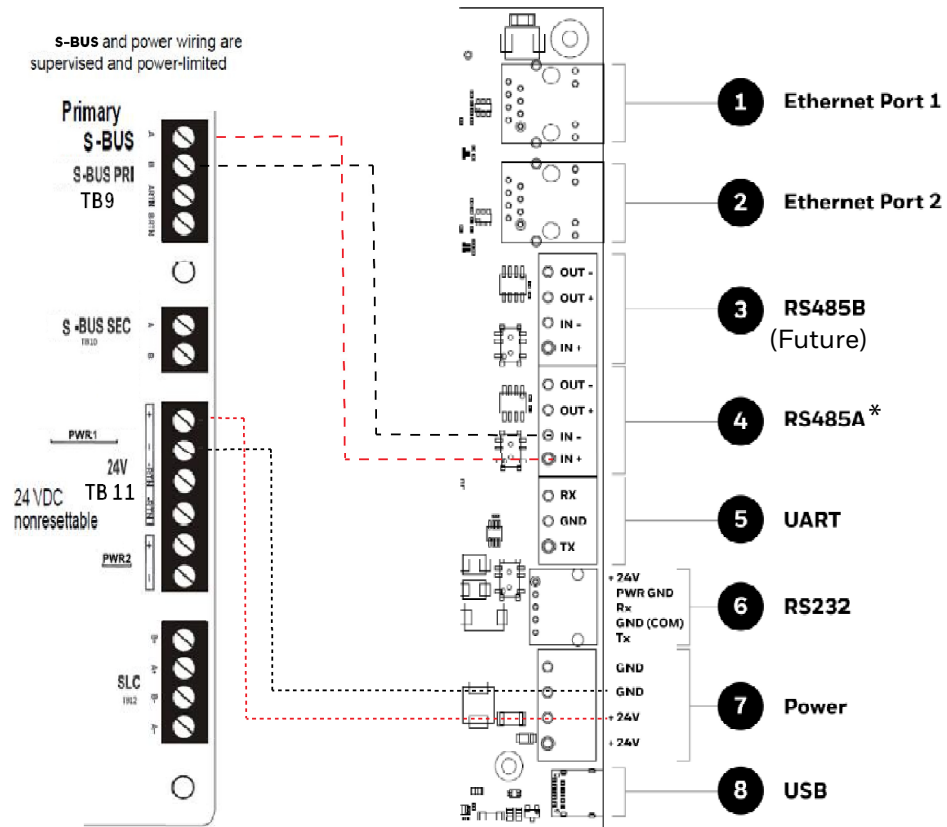
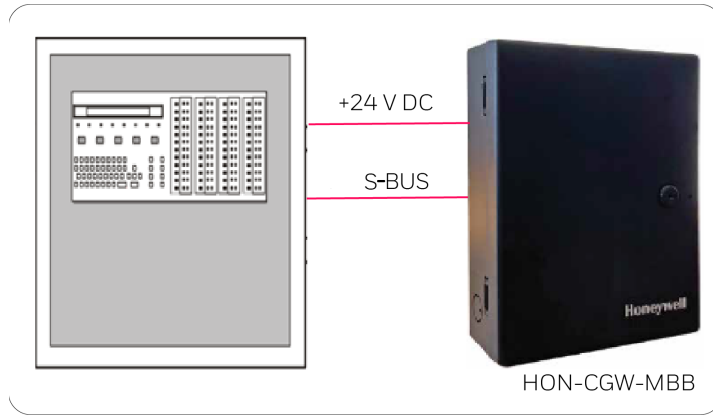
In the power supply port (labeled 7 in the [Figure C.2](#)):

- Connect the Red wire to the +24V pin.
- Connect the Black wire to the Gnd pin.

On the Panel Side

In the power board of the panel:

- Connect the Red wire to the +ve pin.
- Connect the Black wire to the -ve pin.



(* For panel connection, use only the RS-485A port)

Figure C.29: Triga Panel: RS-485 Connections

C.13.3 Programming for Annunciator (ANN-PRI)

Programming enables the panel to recognize the CLSS gateway and the annunciator.



CAUTION: BEFORE PROGRAMMING, ENSURE THAT THE ANN-PRI COMMUNICATION CABLE IS CONNECTED WITH THE PANEL.

C.13.4 To Program for Annunciator

Using the keypad on the panel, you select options on the screens.

1. On the panel, press the **Enter** button on the keypad.
2. View the panel screen options.
3. On the keypad, press **7** to select **7 = PROGRAMMING MODE**.
4. Enter the panel's password in the **PROGRAMMING** screen.
The default password is: 00000000
5. Select the panel connected with the gateway, if it is a standalone panel.

OR

Navigate in the list of panels and select the panel connected with the gateway if it is a multi-panel network.

6. Select **1 = MODULE**.
7. Select **2 = ADD MODULE**.
8. Select the module of the gateway from the list.
9. Select the module type.
10. Select **1 = EDIT MODULE** to enter the module details.
11. Follow the on-screen instructions and enter the communication settings.
12. Review the entered details.

C.14 VESDA® Detectors

C.14.1 Connection Options

The gateway operates with VESDA detectors and sends alarm data to users.

Minimum Required Versions

For VESDA-E: All VESDA-E detector versions

For Android App: 1.0.0.2493 (2493)

For iOS App: 0.3.0 (1124)

For the CLSS Gateway: 3.0.4.70

C.14.2 To Use an Ethernet Connection

Using an Ethernet cable the CLSS Gateway and the VESDA detectors are connected.



NOTE: The CLSS Gateway can connect with a VESDA detector or a VESDA Detector Connector.

Before Connecting

1. In the Configuration Computer
 1. Install the VSC Tool (with a valid license) on the Configuration Computer.
 2. Connect the USB ports of the Configuration Computer and the detector with a Type B cable.
2. In the detector:
 - Using the VSC Tool, configure the respective parameters, including the authentication password.
 - Using the VSC Tool, create a connection profile for Ethernet.
 - If detector connector is used, ensure that the detectors are connected with the detector connector.
3. In the CLSS Gateway: Ensure that the gateway is connected with *CLSS Site Manager* via Ethernet or Wireless.

1. On the Gateway Side

Connect the Ethernet cable to the Ethernet port 2 of the gateway.

Refer to [Figure C.2](#) where it is labeled as the Ethernet Port 2. It is the J3 pin on the gateway board.

2. On the Detector Side

Connect the Ethernet cable to the Ethernet port of the detector.

3. Power Connection

The gateway can receive the 24V DC power from an external power supply.



NOTE: The detector's power supply to the gateway must be within +24V DC power.



WARNING: ENSURE THAT THE BATTERY BACKUP CAPACITY OF A CONNECTED SMOKE DETECTOR IS CORRECTLY CALCULATED. POWER THAT THE GATEWAY ALSO WOULD CONSUME SHOULD BE CONSIDERED IN THE CALCULATION.

On the Gateway Side

- Connect the Red wire to the +ve pin of the power supply port.
- Connect the Black wire to the -ve pin of the power supply port.

External Power Supply

- On the Gateway Side

Connect to the power port of the gateway.

Refer to [Figure C.2](#) where the power port on the gateway is labeled as 7. It is the P2 pin on the gateway board.

- On the External Power Supply Side

Connect to the 24V DC external power supply.

Appendix D: Compatible Cellular Modules

The cellular modules offer value-added services for mobile devices connected with the CLSS Gateway.



Figure D.1: A Cellular Module

To know about installing this device onto the gateway, refer to [“Installing a Cellular Module” on page 26](#).

D.1 Operation

The cellular modules are plug-and-play devices, which receive power from the CLSS Gateway and provide a cellular communication path.

D.2 Supported Modules

Table C.1: Modules and Frequencies

| Brand Name | Verizon Cellular Module | AT&T Cellular Module | EU - Cellular Module |
|-------------------|--|--|--|
| Module Name | CCM-VZ-HON | CCM-ATT-HON | CCM-EU |
| Model | LE910-SV1 | LE910B1-NA | LE910-EU1 |
| Supported Regions | North America | North America | Europe |
| Frequency Details | | | |
| 4G bands (MHz) | <ul style="list-style-type: none"> • B2 (1900) • B4 (AWS1700) • B13 (700) | <ul style="list-style-type: none"> • B2 (1900) • B4 (AWS1700) • B5 (850) • B12/B13 (700) | <ul style="list-style-type: none"> • B1 (2100) • B3 (1800) • B7 (2600) • B8 (900) • B20 (800) |
| 3G bands (MHz) | - | <ul style="list-style-type: none"> • B2 (1900) • B5 (850) | - |
| 2G bands (MHz) | - | - | <ul style="list-style-type: none"> B3 (1800) B8 (900) |

D.3 Standards and Codes

RED Directive 2014/53/EU

- Health and Safety of the User
- Electromagnetic Compatibility
- Effective use of spectrum allocated

D.4 Approvals

Supported cellular module details are below:

Model: CCM-ATT-HON

Region: USA

Contains FCC ID: RI7LE910NAV2

Contains IC: 5131A-LE910NAV2

Model: CCM-VZ-HON

Region: USA

Contains FCC ID: RI7LE910SVV2

Contains IC: 5131A-LE910SVV2

Model: CCM-EU

Region: Europe

R&TTE/GCF

12 Clintonville Rd
Northford, CT 06472

(203) 484-7161

140 Waterside Rd
Leicester LE5 1TN, UK

+44 (0) 203 4091779

Honeywell